UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

Protecting Journalism Sources in the Digital Age

UNESCO Series on Internet Freedom

UNESCO Series on Internet Freedom

UNESCO has started in 2009 to commission this flagship series publications of Internet Freedom, aiming to explore the changing legal and policy issues of Internet and provide its Member States and other stakeholders with policy recommendations aiming to foster a conducive environment to freedom of expression on the net.

This is the 9th edition of the series, with previous editions presented as below:

Human rights and encryption

The study provides an overview of encryption technologies and their impact on human rights. It analyzes in-depth the role of encryption in the media and communications landscape, and the impact on different services, entities and end users. It highlights good practices and examines the legal environment surrounding encryption as well as various case studies of encryption policies. Built on this exploration and analysis, the research provides recommendations on encryption policy that are useful for various stakeholders

Privacy, free expression and transparency: redefining their new boundaries in the digital age

This study analyzes the interactions between the right to freedom of expression, the right to privacy and the value of transparency in the Internet environment. It covers the legal frameworks and current mechanisms for balancing rights, and presents specific issues, cases and trends. The interplays between multiple players – State actors, Internet users, ICT companies, civil society organizations, the judiciary, security services – are envisaged and recommendations for stakeholders are provided.

Principles for governing the Internet

As the sixth edition in the UNESCO Internet Freedom series, this study encompasses both quantitative and qualitative assessments of more than 50 declarations, guidelines, and frameworks. The issues contained in these documents are assessed in the context of UNESCO's interested areas such as access, freedom of expression, privacy, ethics, Priority Gender Equality, and Priority Africa, and sustainable development, etc.

Countering Online Hate Speech

The study provides a global overview of the dynamics characterizing hate speech online and some of the measures that have been adopted to counteract and mitigate it, highlighting good practices that have emerged at the local and global levels. The publication offers a comprehensive analysis of the international, regional and national normative frameworks, with a particular emphasis on social and non-regulatory mechanisms that can help to counter the production, dissemination and impact of hateful messages online.

Building digital safety for journalism: A survey of selected issues

As technologies develop, so do opportunities as well as threats to journalism. This research explains some of the emerging threats to journalism safety in the digital era, and proposes a framework to help build digital safety for journalists. Examining 12 key digital threats to journalism, ranging from hacking of journalistic communications, through to denial-of service attacks on media websites, it assesses preventive, protective and pre-emptive measures to avoid them. It shows too that digital security for journalism encompasses, but also goes beyond, the technical dimension.

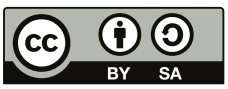
All publications can be downloaded at:
http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/

Julie Posetti

Protecting Journalism Sources in the Digital Age

Published in 2017 by the United Nations Educational, Scientific and Cultural Organization,
7, place de Fontenoy, 75352 Paris 07 SP, France

© UNESCO 2017
ISBN 978-92-3-100219-9



This publication is available in Open Access under the Attribution-ShareAlike 3.0 IGO (CC-BY-SA 3.0 IGO) license (http://creativecommons.org/licenses/by-sa/3.0/igo/). By using the content of this publication, the users accept to be bound by the terms of use of the UNESCO Open Access Repository (http://www.unesco.org/open-access/terms-use-ccbysa-en).

The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The ideas and opinions expressed in this publication are those of the authors; they are not necessarily those of UNESCO and do not commit the Organization.

Author: Julie Posetti
(WAN-IFRA/World Editors Forum/University of Wollongong, Australia)

Academic Researchers: Julie Posetti, France/Australia (Chief Researcher); Marcus O'Donnell, Australia; Carlos Affonso Pereira de Souza, Brazil; Ying Chan, China; Doreen Weisenhaus, China.

Graduate Research Assistants: Federica Cherubini, Angelique Lu, Alice Matthews, Alexandra Waldhorn, Emma Goodman, Farah Wael.

Undergraduate research contributors: Jake Evans, Alexandra Sazonova-Prokouran, Jessica Sparks, Nick Toner, Olivia Wilkinson.

Acknowledgments
The authors would like to thank the University of Wollongong (Australia) as well as UNESCO colleagues, in particular Caroline Hammarberg.

UNESCO thanks Sweden for its support in delivering this publication.

Administrative Support: Ashleigh Tullis

Graphic design: UNESCO
Cover design: UNESCO
Illustrations: UNESCO

Typeset and printed by UNESCO
Printed in France

Table of contents

Foreword 5

Executive summary 7

1. Introduction 11
   - The implications of the digital era 12
   - Background to the study 13
   - Issues and purpose of the research 13

2. Methodology 14
   - Research methods deployed 14

3. Key findings 18
   - Identification of key themes 18
   - Analysis of key themes 19
   - Key themes analysis: Summary 28

4. International Regulatory and Normative Environments 30
   - United Nations actors 31
   - Summary 40

5. Regional instruments of Human Rights Laws and Normative Framework 41
   - European institutions 41
   - The Americas 52
   - Africa 53
   - Asia and The Pacific 55
   - Inter-regional institutions 55
   - Regional Instruments of Human Rights Law: conclusion 56

6. Overviews by UNESCO Region 57
   - Africa 58
   - Arab States 64
   - Asia and the Pacific 67
   - Europe and North America 75
   - Latin America and the Caribbean 94
   - Regional conclusion 101

7. Thematic studies 103
   - Thematic Study 1: The impact of source protection erosion in the digital age on the practice of investigative journalism globally 103

Thematic Study 2: How a State with one of the world's oldest and constitutional legal source protection framework is responding and adapting to emerging digital threats 112
Thematic Study 3: Towards an international framework for assessing source protection dispensations in the digital age 120

8. Gender dimensions arising 134

9. Protecting Journalism Sources in the Digital Age: Conclusion 136

10. Recommendations 137

11. References 140

Appendices 187
Appendix 1: List of experts accessed for qualitative interviews 187
Appendix 2: List of Review Panel Members 191

Foreword

UNESCO is pleased to release this comprehensive study of changes that impact on legal frameworks that support protection of journalistic sources in the digital age. This research responds in part to a UNESCO resolution by the 38th General Conference held in 2015 as well as the CONNECTing the Dots Outcome Document adopted by our 195 Member States that same year. More specifically, the present publication was elaborated in an effort to address option 6.2 of the Outcome Document which recommends that UNESCO "recognize[s] the need for enhanced protection of the confidentiality of sources of journalism in the digital age".

In accordance with this mandate, UNESCO has developed a new approach to Internet and freedom of expression issues regarding safety, privacy, transparency, encryption, hate speech, radicalization and source protection. This is the framework of Internet Universality, and the Internet governance principles of Human Rights, Openness, Accessibility, and Multi-stakeholder Participation. The protection of confidentiality of journalists' sources relates especially to the right to freedom of expression (and the correlatives of press freedom and access to information), and the right to privacy.

While the rapidly emerging digital environment offers great opportunities for journalists to investigate and report information in the public interest, it also poses particular challenges regarding the privacy and safety of journalistic sources. These challenges include: mass surveillance as well as targeted surveillance, data retention, expanded and broad anti-terrorism measures, and national security laws and over-reach in the application of these. All these can undermine the confidentiality protection of those who collaborate with journalists, and who are essential for revealing sensitive information in the public interest but who could expose themselves to serious risks and pressures. The effect is also to chill whistleblowing and thereby undermine public access to information and the democratic role of the media. In turn this jeopardizes the sustainability of quality journalism.

The present research provides a comprehensive review of developments that can impact on the legal frameworks that support protection of journalistic sources. Interviews, panel discussions, thematic studies and a review panel ensured the input of legal and media experts, journalists and scholars. This in-depth study thus seeks to assess the evolution of protective legal frameworks over the eight years from 2007-2015, and provides recommendations for the future of journalistic source protection.

The study found that the legal frameworks that protect the confidential sources of journalism are under significant strain in the digital age. This context is leading journalists to adapt their work methods in an effort to shield their sources from exposure. A majority of the States examined have protections for journalistic sources which now merit revision and strengthening.

A further finding is that all stakeholders have a crucial role to play in the introduction, development or updating of better legal safeguards for all acts of journalism, including for whistleblowers. The research also provides recommendations on journalistic source protection, starting with independent oversight on surveillance and data retention, through to the development of education and training programs in digital safety.

A major output of the study is an 11-point assessment tool for measuring the effectiveness of legal source protection frameworks in the digital era. In this way, the research serves as guidance for UNESCO, Member States and other stakeholders to promote and implement more protective frameworks for the confidentiality of journalistic sources. We further hope that this publication will prove valuable in framing the debate on the new forms of journalism and in encouraging public understanding of these issues.

This research is published as part of a publications series on Internet Freedom that was begun in 2009 and that has strived to develop an Internet Universality framework.

The work for the study was conducted for UNESCO by WAN-IFRA, the global news publishing association that houses the World Editors Forum (WEF). UNESCO would like to thank WAN-IFRA and the author, Julie Posetti, affiliated with the University of Wollongong (Australia), as well as the other academic researchers, research assistants, experts, journalists, lawyers and other interviewees who have contributed to the production of the text.

Frank La Rue

Assistant Director-General
for Communication
and Information

Executive summary

This Study, which covers 121 UNESCO Member States, represents a global benchmarking of journalistic source protection in the Digital Age. It focuses on developments during the period 2007-2015.

The legal frameworks that support protection of journalistic sources, at international, regional and country levels, are under significant strain in 2015. They are increasingly at risk of erosion, restriction and compromise - a development that is seen to represent a direct challenge to the established universal human rights of freedom of expression and privacy, and one that especially may constitute a threat to the sustainability of investigative journalism.

In many of the countries examined in this Study, it was found that legal source protection frameworks are being actually or potentially:

- Overridden by national security and anti-terrorism legislation
- Undercut by surveillance – both mass and targeted
- Jeopardised by mandatory data retention policies and pressure applied to third party intermediaries - like ISPs, telcos, search engines, social media platforms - to release data which risks exposing sources
- Outdated when it comes to regulating the collection and use of digital data, such as whether information recorded without consent is admissible in a court case against either a journalist or a source; and whether digitally stored material gathered by journalistic actors is covered by existing source protection laws.
- Challenged by questions about entitlement to claim protection - as underscored by the questions: "Who is a journalist?" and "What is journalism"?

Several of these categories intersect and overlap, especially in the cases of national security, surveillance and data retention.

These findings are based on an examination of the legal source protection frameworks in each country, drawing on academic research, online repositories, reportage by news and human rights organisations, more than 130 survey respondents and qualitative interviews with nearly 50 international experts and practitioners globally. The study was commissioned as part of the research for an overarching global UNESCO Internet Study, mandated in 2013 by UNESCO's General Conference of 195 Member States in Resolution 52. This mandate called for a comprehensive and consultative study of four dimensions of the Internet as relevant to the remit of UNESCO. Covering access to information and knowledge, freedom of expression, privacy and the ethical dimensions of the information society, this wider study was published as Keystones to foster inclusive Knowledge Societies (UNESCO 2015). Resolution 52 also specifically noted "that privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference" (UNESCO 2013).

This study covers the period 2007-2015, and builds on a 2007 study produced by Privacy International (Banisar 2007).

Of the 121 Member States studied here, developments that impact on source protection in practice, or in potential, have occurred in 84 (69%) countries since 2007, the date of the Privacy International review of source protection laws. However, these changes were not evenly dispersed around the world. The UNESCO region reflecting the most notable developments was the Arab States, where 86% of countries examined demonstrated shifts. Latin America and the Caribbean followed closely behind, with developments in legal protections for journalists' sources recorded in 85% of the States studied. In Asia and the Pacific, 75% of States exhibited notable changes, while 66% of European and North American States also demonstrated developments since 2007. Finally, changes were identified in 56% of African countries examined.

Significant changes in the offline realm of source protection are more prominent in Africa and the Arab States, but they are not limited to these regions. Digital developments were found to be most prevalent in Latin America, Asia, Europe and North America.

While traditional legal frameworks for source protection remain strong in some states, and are progressing in others, they are under significant risk from a combination of developments. These are caused, for the most part, by digital disruption, and by overreach in measures that are introduced in the name of national security or combatting crime. The Study assesses that unless journalistic communications are recognised, surveillance is made subject to checks and balances (both mass and targeted); data retention laws are limited; accountability and transparency measures (applied to both States and corporations) are improved, confidence in the confidentiality of sources could be seen to be weakened. The result could be that much public interest information, such as that about corruption and abuse, will remain hidden from public view.

Many journalists are now significantly adapting their work in an effort to shield their sources from exposure, sometimes even seeking to avoid electronic devices and communications altogether. At the same time, the cost of the digital era source protection threat is very significant - in terms of digital security tools, training, reversion to more labour intensive analogue practices, and legal advice. Regardless, such tactics may be insufficient if legal protections are weak, anonymity is forbidden, encryption is disallowed, and sources themselves are unaware of the risks. The impact of these combined factors on the production and scope of investigative journalism based on confidential sources is significant.

Where source protection is compromised, the impacts can include:

- Pre-publication exposure of journalistic investigations which may trigger cover-ups, intimidation, or destruction of information,
- Revelation of sources' identities with legal or extra-legal repercussions on them,
- Sources of information running dry,
- Self-censorship by journalists and citizens more broadly.

If confidential sources are to confidently make contact with journalists, this Study proposes five conditions for consideration:

- Systems are put in place for transparency and accountability regarding data retention policies and surveillance (including both mass surveillance and targeted surveillance) – as recommended by the UN General Assembly,
- Steps are taken by States to adopt, update and strengthen source protection laws and their implementation for the digital era,
- Training is provided to journalistic actors in regard to digital safety and security tactics,
- Efforts are made to educate the public and sources in Media and Information Literacy, including secure digital communications,
- There is recognition of the application of source protection laws to acts of journalism that encompass digital reporting processes (e.g. phone calls, emails, messaging apps, and hand written notes), along with published content – both digital and non-digital.

A major recommendation of this study is consideration of an 11-point assessment tool for measuring the effectiveness of legal source protection frameworks in the digital age. The 11 points were developed through consultation with 31 international experts in media law, freedom of expression, ICTs, and investigative journalism practice.

On the basis of this output, a model legal source protection framework should:

1. Recognise the value to the public interest of source confidentiality protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country's constitution and/or national law,
2. Recognise that source protection should extend to all acts of journalism, and across all platforms, services and mediums (of data storage and publication), and that it includes digital data and meta-data,
3. Recognise that source protection does not entail registration or licensing of practitioners of journalism,
4. Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection,
5. Affirm that State and corporate actors (including third party intermediaries) who capture journalistic digital data must treat it confidentially (acknowledging also the desirability of the storage and use of such data being consistent with the general right to privacy),
6. Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources,
7. Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard,
8. Define exceptions as needing to conform to a provision of "necessity" and "proportionality" — in other words, when no alternative to disclosure is possible, when there is greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible,

9. Define a transparent and independent judicial process with appeal potential for authorised exceptions, and ensure that law-enforcement agents and judicial actors are educated about the principles involved,

10. Criminalise arbitrary, unauthorised and willful violations of confidentiality of sources by third party actors,

11. Recognise that source protection laws can be strengthened by complementary whistleblower legislation.

This Study concludes that law-makers, journalists, editors and publishers among others can play an important role in promoting public understanding of these issues, and in advocating for change.

A summary leaflet of this publication is available at: http://www.unesco.org/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/protecting_journalism_sources_in_digital_age.pdf

A summary is also available as a chapter in UNESCO's report World Trends in Freedom of Expression and Media Development, Special Digital Focus, 2015. http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/wtr-special-digital-focus-2015/

1. Introduction

> *"…Privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and…such privacy should not be subject to arbitrary or unlawful interference…"* (UNESCO Resolution on Internet-related issues, November 2013).

Internationally, source protection laws are increasingly at risk of erosion, restriction and compromise in the digital era, a development that can be seen to challenge the rights to freedom of expression and privacy (Article 12; Article 19 UDHR, Article 19 ICCPR 1976).

Journalists rely on source protection to gather and reveal information in the public interest from confidential sources. Such sources may require anonymity to protect them from physical, economic or professional reprisals in response to their revelations. There is a strong tradition of legal source protection internationally, in recognition of the vital function that confidential sources play in facilitating 'watchdog' or 'accountability' journalism. While professional journalistic practice entails multi-sourcing, verification and corroboration, confidential sources are a key component of this practice. Without confidential sources, many acts of investigative story-telling - from Watergate to the major 2014 investigative journalism project 'Offshore Leaks' undertaken by the International Consortium of Investigative Journalists (ICIJ) (Guevara et al, 2014) - may never have surfaced. Even reporting that involves gathering opinions in the streets, or a background briefing often relies on trust that a journalist respects confidentiality where this is requested.

There is a globally established ethical obligation upon journalists to avoid revealing the identity of their confidential sources. In some cases, it is also a legal right, or even a legal requirement. In Sweden, protection of confidential sources is so strong that journalists can be prosecuted for revealing their identities (Hendler 2010). However, in many cases, the legal situation does not grant recognition of such confidentiality and journalists can still be legally compelled to identify their sources or face penalties, prosecution and imprisonment. Exceptions to legal protection might include circumstances involving grave threats to human life, when a journalist is accused of committing a crime, or if s/he witnesses a serious crime. Where the legal line is drawn, and how it is interpreted, varies around the world but the principle that sets confidentiality as the norm, and disclosure as the exception, is the generally accepted standard.

The value to society of protecting the confidentiality of sources is widely recognised as greatly offsetting occasional instances of journalists abusing the confidentiality privilege to, for example, invent sources. Such scandals invariably come to light, and they are strongly condemned by journalists' professional organisations that stress the requirement to only rely on anonymous sources when it is necessary to do so to protect the source from exposure, in the course of public interest journalism. Accordingly, free expression standards internationally uphold the confidentiality principle. This principle shields the journalist directly by recognising their professional obligation not to disclose the identity of the source, and it shields the source indirectly through the journalist's commitment. However, this principle works in practice only if the identity of the confidential source cannot be easily discovered by other means, and if there are limits on the use of identifying information if it does become known.

Journalists do not encourage or condone law-breaking, or unsanctioned leaking, but they do have a duty to consider the public interest significance of publishing the resulting

information, and in maintaining confidentiality accordingly, in order not to jeopardize the flow of such information which is vital to accountability journalism.

The need to protect the confidentiality of sources is justified largely in terms of ensuring a free flow of information, especially in regard to information derived from whistleblowers.[1] Without this, a 'chilling effect' is likely, with holders of sensitive information being reluctant to come forward. As another knock-on effect, when media outlets or individuals doing journalism know or suspect that they will be put under pressure to reveal sources, they may become less likely to seek or subsequently use information supplied on condition of confidentiality, with concomitant shrinkage of public interest content as a result.

The implications of the digital era

The current digital environment poses particular challenges to traditional legal protections for journalists' sources. While protective laws and/or a reporter's commitment shielded the identity of sources in the analogue past, in the age of digital reporting, mass surveillance, mandatory data retention, and disclosure by third party intermediaries, this traditional shield can be penetrated.

Technological developments and a change in operational methods of police and intelligence services are redefining the legal classification of privacy and journalistic privilege internationally (Podkowik 2014). In addition, aided by rapid technological advancement, law enforcement and national security agencies have shifted from a process of detecting crimes already committed, to one of threat prevention in the post-September 11 environment. In the digital age, it is not the act of committing (or suspicion of committing) a crime that may result in a person being subject to surveillance, but the simple act of using certain modes of communication – such as mobile technology, email, social networks and the Internet (Podkowik 2014; Banisar 2008). As a result, journalistic communications are increasingly being caught up in the nets of law enforcement and national security agencies as they trawl for evidence of criminal activity, terrorism and national security threats, and conduct leak investigations.

Parallel to these digital developments, over the past eight years increasingly restrictive anti-terrorism and national security legislation has been enacted, actually or potentially overriding existing legal protections, including 'shield laws' (see definitions and discussions of these key terms in section 4.1 below). This arises from moves to broaden the scope of 'classified' information and exceptions to coverage, and to criminalise all disclosure of 'secret' information (including in some cases, the publication thereof) irrespective of public interest or whistle-blowing considerations. The result of the increasing risk to both journalists and their sources is a further constraining, or "chilling", of public interest journalism dependent upon confidential sources.

In this digital and security-driven context, it becomes important to extend legal source confidentiality protection to all acts of journalism, not just to issues of identification after the publication of content based on confidential communications, but also to related prior

1 Martin (1983) describes whistleblowing as disclosure by an employee of his (sic) employer's improper activities and whistleblowers as "…merely ordinary employees who feel so troubled by their employer's conduct that they feel compelled to take action" (Martin, M "Protecting the Whistleblower from Retaliatory Discharge", 16 U. Mich. J.L. Reform 727 (1983) p1. Available at: http://scholarship.kentlaw.iit.edu/fac_schol/372). Whistleblowing may, however, be wider than this, covering public interest issues more broadly than employers' conduct.

digital reporting processes and journalistic communications with sources. Additionally, it is important to debate which journalistic actors qualify for source protection in the digital era – and where there is a need to answer questions like 'Who can claim entitlement to source confidentiality protection laws?'

There are also new questions now facing courts, legislators, media lawyers and journalists. In the analogue era, these were: 1) Can a journalist be forced to reveal the confidential source of published information by a court? 2) Can journalists and news organisations be the subject of targeted surveillance and search and seizure operations? Now, the key questions are increasingly: 1) Do the processes of automatically intercepting and collecting communications through mass surveillance and mandatory data retention which enable subsequent analysis via technologically advanced tools (e.g. Programs that give intelligence agencies access to third party intermediary data stores) constitute a breach of recognition of a right to withhold the identity of sources? 2) Can the effects of such potential interference be minimised or limited through introducing or updating legal source protection frameworks that engage with these challenges? It is the new implications of the digital age that are the main focus of exploration in this study

1.1. Background to the Study

As elaborated later in these pages, the issue of confidentiality of journalists' sources has become a subject of attention within the United Nations. In particular, in November 2013, a UNESCO Resolution mandated the Organisation to undertake a comprehensive study on Internet-related issues. It declared that: "Privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference" (UNESCO 2013). The research contained in this publication fed into the comprehensive study, and is published here in elaborated detail.

1.2. Issues and purpose of the research

The purpose of this Study is to provide quantitative data and qualitative analysis around the world linked to protection of journalists' sources in the digital age (UNESCO: 2014 a). As indicated earlier, its findings have informed the overarching global UNESCO Internet Study (UNESCO: 2014 b; UNESCO: 2015).

The research was conducted by WAN-IFRA, the global news publishing association that houses the World Editors Forum (WEF). The author, Julie Posetti, led the project as WAN-IFRA Research Fellow and WEF Research Editor, with the support of the University of Wollongong, Australia.

2. Methodology

2.1. Research methods deployed

A combination of quantitative and qualitative methodologies was adopted for this study.

i. Structuring the research

An eight-year-old report commissioned by Privacy International called *Silencing Sources: An International Survey of Protections and Threats to Journalists'* Sources (Banisar 2007) was intended to be used as the baseline data set for this study, which was commissioned in mid-2014. However, this approach proved complex, as the 2007 report did not provide a complete public data set.

As a result, the researchers applied a process of 'datafication' to the 2007 report. This process involved hand-mining and keyword searching the document to a) identify every country mentioned in the report and b) establish which countries required additional research to strengthen the available data, thereby enabling an updated benchmarking of the 2007 research. The result was the development of an Excel database that listed each country identified in the 2007 report, along with the different kinds of legal protections applicable globally (e.g. constitutional protections, state-based laws, memoranda of understanding).

There were 124 territories identified through the 'datafication' of the Privacy International report (see section 14.1, Appendix i). The limitation of the research to UNESCO Member States reduced the number of countries selected for examination in this Study to 121. It is this sub-set of countries (see section 14.2, Appendix ii), which constitutes the focus for the research presented here.

ii. Environmental Scan

Once the initial data set was established, each country was assigned to a researcher or research assistant, according to language capacity, for commencement of a qualitative mapping exercise, known as an Environmental Scan. In total, there were five academic researchers commissioned to work on this project, along with 11 research assistants. The languages spoken by the researchers also totalled 11: English, Chinese, Portuguese, Spanish, French, Italian, Russian, Arabic, Vietnamese, Tagalog and German. Where countries were assigned to researchers without relevant language skills, the research was conducted targeting English language sources and replicating the search in a second language where possible. The process of undertaking the Environmental Scan involved:

a. Preparing a literature review (focused on scholarly books, journals and major reports)

b. Online searches of legal, legislative, and relevant NGO databases in each country

c. Online searches of news websites

d. Contacting WAN-IFRA member organisations and affiliates for input

e. Contacting sources in countries

Data collection began on August 1st 2014 and ended on July 20th 2015, when the study was submitted to UNESCO.

Issues arising

There are two important observations to make about the efficacy of the Environmental Scan process when applied globally:

a. In some countries there are issues with availability of information, resulting in limitations in terms of what data could be collected

b. In some contexts there is limited information that is published online, which further constrained the research in all 121 countries.

iii. Preliminary Analysis of country data

Once each country was examined via the Environmental Scan process, the assigned researcher or research assistant produced a 'country overview', identifying any developments relevant to confidential source protection that had occurred in the legal/regulatory/judicial/journalistic environment of that country regarding source protection since 2007, and noting specific digital dimensions. This allowed the author and research assistants to then code the documents produced to further narrow the data corpus to a narrower subset of countries where developments had been identified since 2007.

Ultimately, developments pertaining to legal protections for journalists' sources were recorded in 84 out of the 121 countries (69%) studied. These countries were then divided into UNESCO regional groups, as follows:

i. Africa

ii. Arab States

iii. Asia and the Pacific

iv. Europe and North America

v. Latin America and the Caribbean

iv. Surveys

A set of online survey questions (see 14.4, Appendix iv) was developed by the author, in consultation with academic members of a Review Panel that was set up to assist this Study (see below, Posetti 2014a). These questions were qualitative in nature and designed to engage members of the journalistic, academic, legal, freedom of expression and online communities globally. Specifically, they were asked to: pinpoint shifts in the legal and regulatory environment pertaining to source protection since 2007; identify key experts/actors for future qualitative interviews; and suggest potential case studies. This survey was launched in October 2014 and it continued until January 2015.

The relevant results of an earlier online survey, developed by the author, and launched during the World Editors Forum (WEF) in Turin (Italy) in June 2014, were synthesised with the data from the survey (as described above) distributed in connection with this UNESCO-commissioned Study. The earlier WEF survey targeted editors and investigative journalists,

and it was designed to feed a submission to the over-arching UNESCO Internet Study. It asked for evidence of the impact of the 'Snowden-Effect' on newsrooms globally, in terms of changes in training and practice in reference to source protection, along with broader digital safety issues (Posetti 2014b). The results of the WEF survey usefully expanded the corpus of data examined in this Study as regards the impacts on investigative journalism, and editorial processes and practices, related to challenges posed to legal source protection frameworks in the digital era.

Further, relevant survey data from the over-arching UNESCO Internet Study Survey was provided to the author for examination. Question number 9 of that survey asked: "To what extent do laws protect digitally interfaced journalism and journalistic sources?" (UNESCO 2014b). The author analysed these responses and synthesised the data with that flowing from the two surveys referenced earlier, to produce a complete data set.

In addition to the issues identified in reference to the Environmental Scan process, it is acknowledged that the online nature of the surveys may have discouraged some participants, particularly in light of the subject matter. It is possible that some potential participants may have been concerned about the monitoring and interception of their online communications and therefore elected not to take part in the survey.

Nevertheless, 134 people from 35 countries - representing every UNESCO region - responded to the combined surveys. The survey data was scanned for evidence of changes to legal source protection frameworks, and digital dimensions, which had not been captured in the Environmental Scan process. Such relevant data was used to augment the regional overviews presented below, assist in the identification of expert actors, and in the development of the thematic studies.

v. Qualitative interviews

Dozens of key actors with legal, journalism, and freedom of expression expertise were identified through the Environmental Scan and survey processes. Ultimately, 49 interviewees were selected from 22 countries (see 14.5, Appendix v) on the basis of relevant expertise, and with the goal of achieving regional and gender balance. The author developed nine key qualitative questions to be put to each expert actor for consistency (See 14.6, Appendix vi). Long form, semi-structured qualitative interviews were then conducted by the researchers and research assistants (as assigned in accordance with language capacity), with the selected interviewees. These interviews were conducted via telephone, Skype, email and face-to-face between November 2014 and March 2015. They were recorded, transcribed and coded before being analysed by the author. These interviews served the purpose of deepening the research and forming the foundation of the thematic studies.

vi. Panel Discussions

The author convened two panel discussions on this research during its final phase. The first panel, staged in Washington DC during the World Editors Forum in June 2015 (Greenslade 2015; Posetti 2015d), featured the author and the following experts:

1. Gerard Ryle (Executive Director, International Consortium of Investigative Journalists)
2. Charles Tobin (US attorney specialising in source protection)

3. Amy Mitchell (Director of Journalism Research, Pew Research Centre)

4. Guy Berger (Director of Freedom of Expression and Media Development, UNESCO)

The second panel convened to discuss this Study was hosted jointly by the London Foreign Press Association and the Frontline Club in London, in July 2015 (Churchill 2015). The panellists were:

1. Jonathan Calvert (Editor, Insight, The Sunday Times)

2. Gavin Millar QC (Barrister specialising in media law, including source protection)

3. Jeremy Myers (BBC Internet Research Specialist)

4. Julie Posetti (Author of this study Protecting Journalism Sources in the Digital Age; WAN-IFRA; University of Wollongong)

The contributions of the panellists during both sessions were leveraged to update and strengthen this Study's analysis during the final phase of research. Subsequent presentations of the draft research during 2015 at the Stockholm Internet Forum and the Internet Governance Forum elicited comments from a further range of participants from other parts of the world, and this feedback has enriched the published version of this study.

vii. Thematic Studies

Many potential case studies were identified in the Environmental Scan and survey processes. Ultimately, three thematic studies were selected for in-depth analysis to ensure representation of key issues and reflection of regional and linguistic diversity. The thematic studies draw on the detail of 134 international survey respondents and 49 qualitative interviews (as explained in detail earlier).

The thematic studies featured in this Study are:

a. *The impact of source protection erosion in the digital era on the practice of investigative journalism globally.*

b. *Sweden: How a State with one of the oldest and strongest legal source protection frameworks is responding and adapting to emerging digital transformation and associated threats.*

c. *Model assessment tool for international legal source protection frameworks.*

viii. Review Panel

A Review Panel comprising eight experts in journalism, freedom of expression, ICTs and media law from around the globe was established by the author, in consultation with UNESCO, for the purposes of providing expert advice and feedback on research outputs. Their feedback was incorporated into the Study (See 14.5, Appendix v).

3. Key findings

1. The issue of source protection has come to intersect with the issues of mass surveillance, targeted surveillance, data retention, the spill-over effects of anti-terrorism/national security legislation, and the role of third party Internet companies known as "intermediaries"

2. Legal and regulatory protections for journalists' sources are increasingly at risk of erosion, restriction and compromise

3. 84 UNESCO Member States out of 121 studied (69%) for this report demonstrated developments relevant to the protection of confidentiality of journalistic sources, mainly with actual or potential impact, between 2007 and mid-2015

4. Individual states face a need to introduce or update source protection laws

5. Source protection laws need to cover journalistic processes and communications with confidential sources – including telephone calls, social media, messaging apps, and emails – along with published journalism that depends on confidential sources

6. Transparency and accountability regarding both mass and targeted surveillance, and data retention, are critically important if confidential sources are to be able to continue to confidently make contact with journalists

7. Without substantial strengthening of legal protections and limitations on surveillance and data retention, investigative journalism that relies on confidential sources will be difficult to sustain in the digital era, and reporting in many other cases will encounter inhibitions on the part of potential sources

8. It is recommended to define 'acts of journalism', as distinct from the role of 'journalist', in determining who can benefit from source protection laws

9. To optimise benefits, source protection laws should be strengthened in tandem with legal protections extended to whistleblowers, who constitute a significant set of confidential journalistic sources,

10. Journalists are increasingly adapting their practice in an effort to partially shield their sources from exposure, but steps to limit anonymity and encryption undermine these adaptations.

11. The financial cost of the digital era source protection threat is significant (in terms of digital security tools, training, and legal advice), as is its impact on the production and scope of investigative journalism based on confidential sources

12. There is a need to educate both journalists and citizens in digital safety

13. Journalists and others who rely on confidential sources to report in the public interest may need to train their sources in secure methods of contact and information-sharing

3.1. Identification of key themes

The data collated via the Environmental Scan process and qualitative interviews, many of which are referenced later, confirmed the existence of five key overlapping and inter-related

trends affecting the legal protection of journalists' sources in the digital age. These themes are visible in many legislative changes and incidents affecting journalists, as noted in Part 7 below. They are also reflected in the deliberations of regional courts, such as the European Court of Human Rights. It emerges from all these sources that the issue of confidentiality of journalistic sources in the digital age is bound up with:

i. The 'trumping effect' of national security/anti-terrorism legislation

ii. The role of mass surveillance and targeted surveillance in undercutting legal protections

iii. The role of third party intermediaries and data retention

iv. Changes in entitlement to protection – Who is a journalist?/What is journalism?

v. Additional categories: Two other sub-themes emerged from the data.

   – Other digital dimensions (e.g. seizure of digital equipment; threats to anonymity and encryption)

   – Non-digital developments in source protection (e.g. legislative and case law developments not pertaining to the digital environment)

3.2. Analysis of key themes

i. The 'trumping effect' of national security/anti-terrorism legislation

In 2007, Banisar (p64) noted that: "A major recent concern…is the adoption of new anti-terrorism laws that allow for access to records and oblige assistance. There are also problems in many countries with searches of newsrooms and with broadly defined state secrets acts which criminalise journalists who publish leaked information".

The problem has grown in the intervening years, as a parallel to digital development, and occurs where it is un-checked by measures designed to preserve fundamental rights to freedom of expression and privacy, as well as accountability and transparency. In practice, this leads to what can be identified as a 'trumping effect', where national security and anti-terrorism legislation effectively take precedence over legal and normative protections for confidential journalistic sources (see Campbell 2013). Further, the classification of information as being protected by national security or anti-terrorism legislation has the effect of increasing the reluctance of sources to come forward.

One particular risk is signalled in a 2008 Council of Europe (CoE) report that stated: "Terrorism is often used as a talisman to justify stifling dissenting voices in the way that calling someone a communist or capitalist were used during the Cold War" (Banisar 2008). According to the COE report, following the 2001 terrorist attacks, many European countries adopted new laws or expanded the use of old laws to monitor communications.

Further perspective on the issue has come from Gillian Phillips, Director of Editorial Legal Services of *The Guardian* who has specifically referenced the implications of governments invoking national security and anti-terrorism measures that interfere with protections for journalists and their sources. Calls for unlimited monitoring and use of modern surveillance

technologies to access all citizens' data, directly challenge journalists' rights to protect their confidential sources, she said (Nolan 2015)

Interviewed for this study, the Director of the Centre for Law and Democracy in Canada, Toby Mendel, said that the main issue is the redefinition of national security in the current climate. "The problem is not so much new rules…but a changing understanding of national security. In particular, when national security becomes equated with the risk of terrorist actions, which can theoretically be undertaken by anyone, the issue becomes far more generalised, and so the risk to source protection becomes far more serious" (Mendel 2014).

Privacy International's Tomaso Falchetta, also speaking to this study's researchers, highlighted a major problem with regard to the impact of anti-terrorism and national security legislation on journalistic source protection:

> …*Most laws regulating interception and surveillance do not specifically recognise additional rights for journalists. This is particularly so with regards to counter-terrorism legislation that provides for expansive powers of state surveillance without making provisions for protection of journalists' sources. Traditional national security laws and new counter-terrorism laws adopted in numerous countries give authorities extensive powers to demand assistance from journalists, intercept communications, and gather information.* (Falchetta 2015)

Falchetta also observed that, in many countries, journalists are held liable for the publication of information that they have received when it is judged to be in violation of state secrets acts or criminal codes.

While anti-terrorism legislation could be justifiably used in limited cases to override source protection laws, the existence of arbitrary or broad nature of such laws can put journalistic source confidentiality at risk. This complexity is evident in Australia, where national security and anti-terrorism grounds have been invoked to classify information on asylum seeker arrivals and detention, requiring most journalism undertaken on boat arrivals and immigration detention centres to be dependent upon confidential sources. However, as elucidated later in this study, revelation of any such classified information has now been criminalised (Farrell 2015b), exacerbating the chilling effect. Journalists have been reported to the Australian Federal Police by Australian government agencies with requests that the police assist with identifying the sources of the leaks (Farrell 2015a).

Like other experts interviewed about themes for this study, USA journalist and press freedom advocate Josh Stearns acknowledged that there are, in limited circumstances, security reasons for compelling journalists to reveal their sources. He cautioned, however, that "too often the blanket of national security is thrown over things that probably aren't a good fit or it is used too expansively" (Stearns 2014)

A report by *The Guardian* in 2015, based on files leaked by Edward Snowden, highlighted the potential controversy in this area. It stated that that a UK Government Communications Headquarters (GCHQ) information security assessment had listed "investigative journalists" alongside terrorists and hackers in a threat hierarchy (Ball 2015).

In Africa, *ARTICLE 19*'s Henry Maina told the researchers that journalists and bloggers are frequently targeted in the context of national security measures (Maina 2015). Former Special Rapporteur on Freedom of Expression at the Inter-American Commission on Human Rights, Dr Catalina Botero, told this study that the role played by investigative journalism

in the fight against terrorism and organised crime is being undermined in Latin America through deployment of national security laws to the detriment of source protection:

> *You need to protect journalists in order to fight organised crime because you need [their work] to know what's going on. Sometimes in the Americas, journalists are more and better informed than the authorities. So you need them to fight against organised crime and at the same time you are using these kinds of laws to threaten them. We're killing one of the most important tools that governments need to fight organised crime, and you're not winning anything because spying on journalists is not going to give you any tool to fight against organised crime*. (Botero 2015)

She stated that some governments use tools to block and threaten and spy on journalists. "Not because of security reasons, but because of the need to control what's going on in the public sphere" (Botero 2015).

Globally, these issues point to the need for law reform according to Media Legal Defence Initiative CEO Peter Noorlander. "Existing national security and search and seizure laws should be amended to strengthen source protection," he told this study (Noorlander 2015).

Other issues related to national security impact on whether a society provides for anonymity and encryption, which are enablers of the right to privacy, and which each have great relevance to the confidentiality of journalistic sources. Linked to these are real-name registration systems for electronic communication, which potentially expose reporters and their communications with sources to scrutiny. There is also a potential chilling effect on sources who may prefer to make contact with reporters via anonymous or pseudonymous accounts. This presents risks and difficulties for journalists trying to interact with confidential sources online – sources who may choose to make contact via journalists' personal social media accounts, including private and direct messaging. The same applies to the legal regime concerning encryption, which is also sometimes affected by national security considerations.

ii. The role of mass surveillance and targeted surveillance in undercutting legal protections

This theme is highlighted by a range of scholars (Fuchs 2013; Eubanks 2014; Giroux 2015) who have warned that surveillance is a broader problem than the impingement of individual privacy. Adrejevic (2014) has argued that it represents a fundamental alteration to the power dynamics of society:

> …*Surveillance should be understood as referring to forms of monitoring deeply embedded in structural conditions of asymmetrical power relations that underwrite domination and exploitation.*

As discussed throughout this study, protection of journalistic sources is undercut if information leading back to sources is swept up through both mass surveillance and unchecked targeted surveillance deployed by States and other actors. Different kinds of physical surveillance have historically impacted on source protection, but digital data has enabled a higher magnitude of surveillance, and the advent of cheap storage and processing power makes bulk surveillance feasible and far-reaching. Director of the Canadian-based Centre for Law and Democracy, Toby Mendel told this study that digital surveillance undercuts source protection because it gets around legal controls on exposing

sources via indirect means (Mendel 2014). *ARTICLE 19*'s Henry Maina told this study there were some countries where the deployment of surveillance techniques was a means of intercepting information that can be used to incriminate reporters (Maina 2015). Experts interviewed for this study indicated that surveillance could be legitimate, and pointed to the "Necessary and Proportionate" conditions put forward by civil society groups[2], but expressed concern about cases when there was a lack of legality, independent oversight, transparency or consideration for journalistic confidentiality.

Definitions

Mass surveillance can be defined as the broad, arbitrary monitoring of an entire or substantial fraction of a population (EFF 2015). According to former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion, Frank La Rue, States can achieve almost complete control of telecommunications and online communications "…by placing taps on the fibre-optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition…" (UNGA HRC 2013).

Privacy International's Tomaso Falchetta described the particular risks of mass surveillance to researchers on this study: "Mass digital surveillance is inherently untargeted, thereby collecting all types of information, often greater than those obtained by other legal means. The surveillance is likely to result in the interception of information about other sources, research on pending stories, and the personal life of the journalist" (Falchetta 2015).

A report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ben Emmerson, has outlined that States can gain access to the telephone and email content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites. "All of this is possible without any prior suspicion related to a specific individual or organisation. The communications of literally every Internet user are potentially open for inspection by intelligence and law enforcement agencies in the States concerned" (UN Doc A/69/397).

There is also concern about the extent of targeted surveillance, according to Emmerson's report: "Targeted surveillance…enables intelligence and law enforcement agencies to monitor the online activity of particular individuals, to penetrate databases and cloud facilities, and to capture the information stored on them" (UN Doc A/69/397).

In 2013, the Monk School of Global Affairs' Citizen Lab research group at the University of Toronto discovered command and control servers for FinFisher software (also known as FinSpy) backdoors, in a total of 25 countries, including 14 countries in Asia, nine in Europe and North America, one in Latin America and the Caribbean, and one in Africa (Marquis-Boire et al. 2013). This software is exclusively sold to governments and law enforcement agencies (Blue 2014).

The practice of 'outsourcing' the interception of citizens' communications to allied countries' national security agencies, in order to avoid domestic privacy and freedom of expression laws, may heighten the risks for journalistic source protection.

Additionally, several experts interviewed for this Study pointed out the lack of transparency connected to surveillance practices that target journalists, or catch them in the net.

2 https://necessaryandproportionate.org/

Belgian Media Law professor Dirk Voorhoof told this Study's researchers: "When it comes to monitoring online communications, the practices that are breaching the rights (associated with) protection of journalists' sources almost become invisible, and these practices are often to be situated in the nearly invisible actions of security and intelligence services". He described the lack of transparency, and associated lack of enforcement of source protection laws in the digital environment as a problem for democracy (Voorhoof 2015).

Trends in surveillance of journalists and their communications

A 2008 Council of Europe report (Banisar 2008) detailed what it described as a "worrying trend in the use of both authorised and unauthorised electronic surveillance to monitor journalists by governments and private parties to track their activities and identify their sources". According to the report, most such incidents are not related to countering terrorism but they are authorised under the broad powers of national laws or undertaken illegally, in an attempt to identify the sources of journalistic information.

These laws expand surveillance in a number of ways, according to the CoE study, such as:

1. Extending the range of crimes that interception is authorised for;
2. Relaxing legal limitations on approving and conducting surveillance including allowing for warrantless interception in some cases;
3. Authorising the use of invasive techniques such as Trojan horse and remote keystroke monitoring to be used;
4. Increased demand for identification of users of telecommunications services.

One case of the direct undercutting of confidential source protection by mass surveillance came in July 2015, in the context of a German parliamentary investigation into the surveillance of German citizens in 2011. During the course of questioning, a German intelligence chief revealed that Der Spiegel journalists had also been under surveillance and that an official from the service of an ally had revealed the identity of one of the journalists' confidential sources to the German government (Tapper 2015).

Documents linked to Edward Snowden, published by *The Guardian* in 2015, posited that the UK's GCHQ (Government Communications Headquarters) had syphoned emails from some of the world's top news organisations – the BBC, *The Guardian*, *Le Monde*, Reuters, *The New York Times* and *The Washington Post* among them – for internal distribution (Ball 2015).

Meanwhile, a US editor who responded anonymously to the first of three surveys connected to this study (Posetti 2014d) argued that mass surveillance meant that newsrooms could not protect the anonymity of sources anymore, and that sources could also expose themselves through their electronic communications.[3] Similar concerns were expressed by Indonesian investigative journalist with TEMPO magazine, Wahyu Dhyatmika, and Pakistani investigative journalist Umar Cheema. In the Philippines, investigative journalist Marites Danguilan-Vitug, a co-founder of that country's Centre for Investigative Journalism, told the researchers that she believed her phone had been bugged, causing her to introduce additional security measures.

3 Such concerns have led to the defensive alteration of journalistic practices. See Thematic Study 1, and Part 9.e of this Study.

Founder of the Arabic Media Internet Network Daoud Kuttab told this study that he now operates on the assumption that everything he does is "being watched" and that governments and security services have access to his communications, and those of many other media actors in his region.

Mexican journalist, and World Editors Forum Special Adviser on Journalists' Safety, Javier Garza Ramos said that journalists now operated under the assumption that they were under surveillance. (Garza 2015).

Also in an interview for this study, the editor of a major newspaper in the People's Republic of China (PRC), said surveillance undermined his confidence in his ability to protect his sources (Yuan Zhen[4] 2015).

US journalist Josh Stearns told this study that traditionally, journalists sought to protect sources through shield laws[5], and that many of these were now dated (Stearns 2014).

According to Polish law academic Jan Podkowik (2014), surveillance undertaken without a journalist's consent should be considered as an act of interference with the protection granted by Article 10 of the European Convention on Human Rights. He proposed in a 2014 paper that interference with journalistic confidentiality by means of secret surveillance should be recognised at least as equally onerous (or even more onerous) as searches of a home or a workplace. "… it seems that in the digital era, it is necessary to redefine the scope of the protection of journalistic privilege and to include in that scope all the data acquired in the process of communication, preparation, processing or gathering of information that would enable the identification of an informant," Podkowik wrote.

iii. The role of third party intermediaries and data retention

A third theme that emerges from the literature, surveys, expert interviews and legal developments is that of data retention by third parties. Compounding the impacts of surveillance on source protection and confidential source-dependent journalism globally is the interception, capture and long term storage of data by third party intermediaries[6]. If ISPs, search engines, telcos, and social media platforms, for example, can be compelled to produce electronic records (stored for increasingly lengthy periods under mandatory data retention laws) that identify journalists' sources, then legal protections that shield journalists from disclosing confidential sources may be undercut by backdoor access to the data.

A 2014 UN Office of the High Commissioner for Human Rights Report, *The Right to Privacy in the Digital Age* (see detailed discussion of this report in section 5.1 b below) concludes that there is a pattern of:

> *…increasing reliance of Governments on private sector actors to retain data 'just in case' it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies*

4 This is a pseudonym

5 Shield laws offer journalists the legal right not to disclose their sources

6 In the UNESCO publication *Fostering Freedom Online: The Role of Internet Intermediaries* (MacKinnon et al 2014), the authors cite the Organisation for Economic Co-operation and Development's (OECD) definition of Internet intermediaries as entities that 'bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.' Most definitions of Internet intermediaries explicitly exclude content producers.

and internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate (OHCHR 2014).

Privacy International legal officer Tomaso Falchetta told researchers attached to this study that: "there is a growing trend of delegation by law enforcement of quasi-judicial responsibilities to Internet and telecommunication companies, including by requiring them to incorporate vulnerabilities in their networks to ensure that they are 'wire-tap ready'" (Falchetta 2015). He pointed in this regard to the UN High Commissioner for Human Rights' report on the right to privacy in the digital age (UN doc. A/HRC/27/37, 30 June 2014).

Limited judicial oversight of access to data is also an issue globally.

Mandatory data retention

Increasingly, States are introducing mandatory data retention laws. Such laws require telecommunications and Internet Service Providers to preserve communications data for inspection and analysis, according to a report of the Special Rapporteur on Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (23 September 2014) (UN Doc A/69/397). In practice, this means that data on individuals' telecommunication and Internet transactions are collected and stored even when no suspicion of crime has been raised (EFF 2011).

Australia's Press Council Chair, Professor David Weisbrot has said that mandatory data retention legislation that fails to protect journalistic communications risks "crushing" investigative journalism:

I think that whistleblowers who are inside governments or corporations will definitely not come forward because their confidentiality and anonymity will not be guaranteed. If they came forward, a journalist would have to say 'I have to give you some elaborate instructions to avoid detection: don't drive to our meeting, don't carry your cell phone, don't put this on your computer, handwrite whatever you're going to give me' (Meade 2015)

Senior Lawyer with Australia's Law Institute of Victoria, Leanne O'Donnell, told this study that the country has had no exemption for journalistic communications in data retention policies. She added that there were also no protocols that could assist ISPs, and other companies to determine if official handover requests apply to journalistic communications. There had been, therefore, no legal provision or practical protection for journalistic data, she stated[7] (O'Donnell 2015).

The issue of access to journalistic data raises transparency issues. UK QC Gavin Millar, Chair of the Centre for Investigative Journalism at Goldsmith's University in London, told this study that the process of accessing journalists' data under the Regulation of Investigatory Powers Act (RIPA) in the UK involves judges, but not the journalists (Millar 2015).[8]

Metadata risks

Some of the data collected under these policies is known as metadata. Metadata is data that defines and describes other data. For the ISO (International Organisation for Standardisation) standard, metadata is defined as data that defines and describes other data and processes.

7 See discussion about new data retention legislation in Australia in the regional overviews section of this study

8 See part 9.3.2.c below for further discussion about transparency issues

(ISO/IEC FDIS 11179-1, 2004). In other words, as the Electronic Frontier Foundation's Peter Eckersley has put it, "Metadata is information about what communications you send and receive, who you talk to, where you are when you talk to them, the length of your conversations, what kind of device you were using and potentially other information, like the subject line of your emails" (EFF 2014). Metadata may also include geolocation information.

Advocates of long-term metadata retention insist that there are no significant privacy or freedom of expression threats.[9] However, even when journalists encrypt the content, they may neglect the metadata, meaning they still leave behind a digital trail when they communicate with their sources. This data can easily identify a source, and safeguards against its illegitimate use are frequently limited, or non-existent (Noorlander 2015).

The need to include the metadata attached to journalistic communications in any limitations applied to the reach of data retention laws is also highlighted by the legal and legislative developments, along with a range of associated incidents identified later in this study. The Media Legal Defence Initiative director Peter Noorlander told the researchers that many legislators do not realise the very real threat to privacy and media freedom posed by the collection of metadata (Noorlander 2015). In an interview for this study, the Tow Center's Susan McGregor called for legislation in the USA to declare metadata private because of what it reveals about people's personal lives.

iv. Changes in entitlement to protection – Who is a journalist?/ What is journalism?

These questions are persistent and complex. On the one hand, broadening the legal definition of 'journalist' to ensure adequate protection for citizen reporters (working on and offline) is logical, and in some countries case law is catching up gradually on this issue of redefinition. However, on the other hand, it opens up debates about classifying journalists, and even about licensing and registering those who do journalism - debates that are particularly potent where there is a history of controls over press freedom.

Various scholars (c.f. Russell 2014), journalism organisations (Society of Professional Journalists 2013) and press freedom advocacy groups (Stearns 2013) have all recently recognised this change in the landscape and proposed that sources of journalism should be protected from legal repercussions by whistleblowing laws, for example, and not limiting the protection to journalists alone . In many dispensations without strong press freedom overrides, however, journalists themselves are liable for publication of leaked information, irrespective of source confidentiality issues. In such cases, they too need protection in terms of public interest defences being recognised in law and by the courts. In other words, confidentiality protection as such does not necessarily shield publication, even where it does assist sources to avoid identification. The significance of this is that where there are no other protections to complement confidentiality protection, there can nevertheless be a chilling of disclosures of public interest information.

Many stakeholders have argued in favour of legal protections being defined in connection with 'acts of journalism', rather than through the definition of the professional functions of a journalist. These have bearings on the protection of both journalists and sources in the digital age. In December 2013, the UN General Assembly adopted a resolution which

9 See for example Australian Attorney General George Brandis' defence of that country's data retention policies http://www.skynews.com.au/culture/showbiz/tv/2015/03/23/metadata-grilling-gains-logie-nomination.html

outlined a broad definition of journalistic actors that acknowledged that: "…journalism is continuously evolving to include inputs from media institutions, private individuals and a range of organisations that seek, receive and impart information and ideas of all kinds, online as well as offline, in the exercise of freedom of opinion and expression" (UNGA 2013: A/RES/68/163).

In 2014, the intergovernmental Council of UNESCO's International Program for the Development of Communications (IPDC) welcomed the UNESCO Director-General's Report on the Safety of Journalists and the Danger of Impunity, which uses the term 'journalists' to designate the range of "journalists, media workers and social media producers who generate a significant amount of public-interest journalism" (UNESCO 2014).

Many legal definitions of 'journalist' have been evaluated as overly narrow, as they tend to emphasise official contractual ties to legacy media organisations, may demand a substantial publication record, and/or require significant income to be derived from the practice of journalism. This leaves confidential sources relied upon by bloggers and citizen journalists largely unprotected, because these producers of journalism are not recognised as 'proper journalists', even when their output is clearly public interest journalism. Such definitions also exclude the growing group of academic writers and journalism students, lawyers, human rights workers and others, who produce journalism online, including investigative journalism.

There are many parallels between investigative journalism and the work undertaken by human rights organisations – organisations that depend upon confidential sources for information about human rights abuses. Such organisations now also often publish directly to audiences and are arguably engaged in 'acts of journalism'. This has bearing on a controversy in 2015 in which *Amnesty International* objected to having been a subject of surveillance (*Amnesty International* 2015a, 2015b).

The Arabic Media Internet Network's Dauoud Kuttab does not want to limit entitlement to source protection to recognised journalists, but to extend it to citizens as well (Kuttab 2015). Egyptian Media Studies Professor Rasha Abdullah said that source protection needs to be accessible to a broad range of communications actors: "It should apply to anyone who has information to expose, particularly in the age of digital media" (Abdullah 2014). However, for Arab Reporters for Investigative Journalism's (ARIJ) Rana Sabbagh, "There is a difference between reporting the news, writing an editorial, and being an activist" (Sabbagh 2015). Nevertheless, she stated that: "…credible bloggers who are using reliable documents and are exposing corruption and injustice have to have some form of protection".

USA media lawyer Charles Tobin is also in favour of a broad definition of journalism as a response to the rise of citizen journalists and bloggers (Tobin 2014). In 2013, the USA's Society of Professional Journalists passed a unanimous motion that "strongly rejects any attempts to define a journalist in any way other than as someone who commits acts of journalism". Karen Russell (2014), in her analysis of attempts to define "journalist" in the context of USA shield law debates, argued that: "Shield laws should be designed to protect the process through which information is gathered and provided to the public, not the status of the individual or institution collecting it". She noted that a number of jurisdictions in the USA already define journalism in such a way. In the state of Nebraska, for example, the shield law states "[n]o person engaged in procuring, gathering, writing, editing, or disseminating news or other information to the public" shall be required to disclose a confidential source or information provided by that source in any federal or state proceeding.

In the view of USA journalist Josh Stearns: "we need to look at the acts of journalism rather than defining a particular type of person…defining an act is safer and more consistent with how media is created and consumed today, and (it) provides a stronger basis for protection." He further told this study that: "Even those who are blessed with journalism jobs and would fit all the qualifications that would protect such a person under law may not act in such a way as deserves protection. By orienting around an act, and protection of an act, we then hopefully establish actions that are for the public interest and have all these sets of qualities rather than just protect a person who automatically lumps in and excludes people who should otherwise be included" (Stearns 2014)

Moving the framework to a protection of 'acts of journalism' rather than limiting it to the work of professional journalists is a conceptual shift, according to Stearns in a 2013 report:

> *While there is an emerging consensus on protecting acts of journalism, how we define those acts is contested terrain. It raises questions about whether there is indeed an act of journalism we can differentiate from other acts. Given how much flux exists in the journalism world, how can we create boundaries around an idea while leaving enough flexibility to account for an unknown future?*

Central to these debates is the deployment of a 'public interest test' as a measure for assessing the entitlement for a journalistic actor to claim access to source protection frameworks. The term 'in the public interest'[10], as it applies to acts of journalism, is not clearly defined and it is a complex concept (see discussion in Thematic Study 3). It may, in some cases, have the effect of inadvertently excluding certain acts of journalism from source protection provisions. This concept may need further interrogation in reference to the development of shield laws, and it points to the need for a case-by-case assessment of the specific journalistic acts for which confidentiality is sought.

3.3. Key themes analysis: Summary

The four themes above are the key digital era issues emerging from the research undertaken for this study. They are distinct, though inter-related, themes for understanding the evolving regulatory environment and the regional analyses that follow below. In a nutshell, they are patterns in terms of which: 1) source protection laws are at risk of being trumped by national security and anti-terrorism legislation that increasingly broadens definitions of 'classified information' and limits exceptions for journalistic acts, 2) The widespread use of mass and targeted surveillance of journalists and their sources undercuts legal source protection frameworks by intercepting journalistic communications, 3) Expanding requirements for third party intermediaries to mandatorily retain citizens' data for increasingly lengthy periods of time further exposes journalistic communications with confidential sources 4) debates about digital media actors' entitlement to access source protection laws where they exist, while being more prominent in Western contexts, are intensifying around the world. These themes inform the regional catalogue of developments affecting legal source protection frameworks – including legislative changes, judicial precedents, incidents and revelations –

10 Moore (2007) Argues that public interest journalism has two elements: 1. "…it is as a watchdog, holding the powerful to account, exposing fraud, deceit, corruption, mismanagement and incompetence… This watchdog role is (also) important…because those in power know they're being held to account". 2. "This is the responsibility to inform, explain and analyse. Public- interest journalists find, digest and distil information that helps the public form views and make decisions" (Moore, M "Public interest, media neglect" in *British Journalism Review* (Sage) vol. 18 no.2, June 2007.)

that follow. Also examined below are other digital aspects such as the seizure of technical equipment and legal developments not linked specifically to digital dimensions.

It is relevant to begin examining the way in which international regulations and norms impact on these themes, especially from the vantage point of looking at those developments that have a close bearing on the confidentiality of source protection.

4. International Regulatory and Normative Environments

> *"There is widespread recognition in international agreements, case law and declarations that protection of journalists' sources [are] a crucial aspect of freedom of expression that should be protected by all nations"* (Banisar 2007: p13).

As elaborated later in this study, the United Nations (including UNESCO), Organisation of American States, African Union, Council of Europe, and the Organization for Security and Co-operation in Europe (OSCE) have specifically recognised journalists' right to protect their sources. Further, the European Court of Human Rights (ECtHR) has found in several cases that it is an essential component of freedom of expression.

As Banisar (2007: 13) noted, the international instruments concur that the protection of sources is "indispensable" and a "basic condition for press freedom. Such protection is viewed as necessary to ensure the free flow of information - an essential element of several international human rights agreements. "Without it, the media will not be able to effectively gather information, and provide the public with information, and act as an effective watchdog". The presumption made is that "exceptional circumstances" are required to justify disclosure of journalists' confidential sources. Accordingly, the need for information about the source must be judged as essential, and only in cases where there is a 'vital interest' can disclosure be justified.

The terms of this Study required a review of existing global and regional instruments (including laws, statements and declarations) to identify any changes in law, and within the normative environment, along with an assessment of their digital relevance in 2015.

The global instruments assessed for relevance to source protection are grouped under the jurisdiction of:

- United Nations (including UNESCO)
- European institutions:
  a) The Council of Europe (CoE), including the European Court of Human Rights (ECtHR)
  b) European Union (EU), including the European Court of Justice
- Organisation for Security and Co-operation in Europe (OSCE)
- Organisation for Economic Cooperation and Development (OECD)
- Organisation for American States (OAS)
- African Union (AU)

This study will focus on mapping developments between 2007-2015 that are relevant to journalistic source protection, while identifying emerging digital dimensions in evidence.

4.1. United Nations Actors

a. Resolutions

- *2012: Resolution adopted by the UN Human Rights Council (A/HRC/RES/20/8) on the promotion, protection and enjoyment of human rights on the Internet that recognise the need to uphold people's rights equally regardless of environment*

The resolution affirmed that: "the same rights that people have offline must also be protected online". This represents important support for extending legal source protection provisions for analogue journalistic processes to the digital realm.

- *2012: Human Rights Council resolution (A/HRC/RES/21/12 on the safety of journalists.*

This Resolution stressed "the need to ensure greater protection for all media professionals and for journalistic sources" (UN Human Rights Council, 2012).

- *2013: Resolution adopted by the UN General Assembly (A/RES/68/163) on the Safety of Journalists and Issue of Impunity (2013)*

This resolution acknowledges that "…journalism is continuously evolving to include inputs from media institutions, private individuals and a range of organisations that seek, receive and impart information and ideas of all kinds, online as well as offline, in the exercise of freedom of opinion and expression, in accordance with article 19 of the International Covenant on Civil and Political Rights thereby contributing to the shaping of public debate" (UN GA 2013).

This resolution is directly relevant to this study in two ways: a) It acknowledges shifts in definitions of 'journalism' that are relevant to debates about who is entitled to invoke source protection, and b) it acknowledges the value of journalism to the public interest.

It further noted with appreciation the UN Plan of Action on the Safety of Journalists and Issue of Impunity. In turn, it is significant that the Plan states:

> *Efforts to end impunity with respect to crimes against journalists must be associated with the defence and protection of human rights defenders, more generally. In addition, the protection of journalists should not be limited to those formally recognised as journalists, but should cover others, including community media workers and citizen journalists and others who may be using new media as a means of reaching their audiences.*

- *In November 2013, the 37th session of the UNESCO General Conference passed a Resolution on 'Internet-related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society' (UNESCO 2013).*

This resolution formally recognised the value of investigative journalism to society, and the role of privacy in ensuring that function. "…(P)rivacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference," the resolution reads in part.

- *In December 2013 the United Nations General Assembly (UNGA) adopted a resolution on the Right to Privacy in the Digital Age. (A/C.3/68/167)*

Resolution 68/167 was co-sponsored by 57 Member States and it called upon all States to "… respect and protect the right to privacy including in the context of digital communication. … To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law".

The Resolution expressed 'deep concern'"…at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights".

It also called upon States: "To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law" and "To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data," emphasising the need for States to ensure the full and effective implementation of their obligations under international human rights law (OHCHR 2014).

The General Assembly further requested the United Nations High Commissioner for Human Rights to submit a report on "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale". The Assembly, in line with the 2012 Human Rights Council resolution (UN Doc. A/HRC/RES/20/8), also affirmed: "That the same rights that people have offline must also be protected online, including the right to privacy".

Through its calls to protect the right to privacy, including in the context of digital communications, this UNGA resolution is relevant to source protection. The right to privacy online applies also to journalists, and it can be invoked to support investigative journalism via their dealings with confidential sources. Whistleblowers – a prominent subset of journalists' confidential sources – are more likely to communicate with journalists directly online if journalists can rely on their right to privacy to help shield their professional communications.

- *2014: Resolution adopted by the UN Human Rights Council (A/HRC/RES/27/5) on the Safety of Journalists*

The resolution acknowledged "the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or interception of communications, in violation of their rights to privacy and to freedom of expression".

This observation has direct application to the issues of source protection and the safety of journalists and their sources.

- *December 2014: UN General Assembly Resolution on The safety of journalists and the issue of impunityfreedoms (A/RES/69/185)*

This UNGA resolution is relevant to this study, as it reiterates two observations pertinent to the implications of mass surveillance and questions of defining acts of journalism:

> ***Acknowledging*** *that journalism is continuously evolving to include inputs from media institutions, private individuals and a range of organisations that seek, receive and impart information and ideas of all kinds, online as well as offline, in the exercise of freedom of opinion and expression, in accordance with article 19 of the International Covenant on Civil and Political Rights, thereby contributing to the shaping of public debate* (Reaffirming the 2013 UNGA Resolution 163 above)

> ***Acknowledging*** *also the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance or interception of communications in violation of their rights to privacy and to freedom of expression* (Reaffirming the UN HRC resolution of 2014 above).

b. Reports, recommendations, statements and comments

- *July 2011: Office of the International Covenant on Civil and Political Rights UN Human Rights Committee, General Comment no. 34*

This comment recognises protection of all forms of expression and the means of their dissemination, including electronic and Internet-based modes of expression.

> *…Freedom of opinion and freedom of expression are indispensable conditions…essential for any society. They constitute the foundation stone for every free and democratic society, and form the basis for the full enjoyment of a wide range of other human rights. A free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other Covenant rights. This implies a free press and other media able to comment on public issues and to inform public opinion without censorship or restraint.*

- *2012: Carthage Declaration - participants at the UNESCO World Press Freedom Day conference:*

This declaration highlights the significance of the challenges posed by Internet communications to the maintenance of freedom of expression and privacy rights essential to the practice of investigative journalism.

> *Noting the Report to the Human Rights Council of 2011 by the UN Special Rapporteur for Freedom of Opinion and Expression with respect to access to Internet and the right of all individuals to freedom of expression, including through the Internet (A/HRC/17/27)*

Calls on UNESCO to:

> *Coordinate dialogue among Member States and other stakeholders on the human rights implications of social networks and new media for freedom of expression, privacy, and personal data protection.*

- *June 2013: 'Report of the Special Rapporteur (Frank La Rue) on the Promotion and Protection of the Right to Freedom of Opinion and Expression' to the Human Rights Council (A/HRC/23/40)*

This Report states: "Journalists must be able to rely on the privacy, security and anonymity of their communications. An environment where surveillance is widespread, and unlimited by due process or judicial oversight, cannot sustain the presumption of protection of sources". It further notes: "States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy." (La Rue 2013).

This statement highlights the relationship between the rights to freedom of expression, and access to information and privacy that underpins source protection.

- *In July 2013, the then UN High Commissioner for Human Rights, Navi Pillay spotlighted the right to privacy in protecting individuals who reveal human rights implicated information.*

"[Edward] Snowden's case has shown the need to protect persons disclosing information on matters that have implications for human rights, as well as the importance of ensuring respect for the right to privacy," Pillay said (UN 2013 b). She added that national legal systems must ensure avenues for individuals disclosing violations of human rights to express their concern, without fear of reprisals.

Although the protection of journalistic confidentiality does not necessarily encompass protection of the source's act of disclosure, fear of reprisal is a factor that affects a source's confidence in a journalist's commitment to keep confidentiality. In this way, an increased fear of reprisal can increase the 'chilling effect'.

Pillay declared that the right to privacy, the right of access to information, and freedom of expression are closely linked. "The public has the democratic right to take part in public affairs and this right cannot be effectively exercised by solely relying on authorized information".

This point is relevant to source protection because much investigative journalism is dependent upon 'unauthorised' sources - that is, sources who have not been cleared by government, organisational or corporate agencies to comment.

Pillay also explicitly pointed to the need for people "to be confident that their private communications are not being unduly scrutinised by the State".

The consequence of an absence of such confidence represents a 'chilling effect' on sources that could, in turn, lead to the freezing of the 'information pipe'.

Pillay's statement has added relevance to source protection as Edward Snowden initially made his revelations to Guardian journalist/blogger Glenn Greenwald and The Washington Post as a confidential source (Greenwald 2014).

- *In February 2014, the UN hosted an international expert seminar on the Right to Privacy in the Digital Age (Geneva)*

During this seminar, Frank La Rue (then UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), called for a special United Nations mandate for protecting the right to privacy. "Privacy and freedom of expression are not only linked, but are also facilitators of citizen participation, the right to free press, exercise of free opinion, and the possibility of gathering individuals, exercising the right to free association, and to be able to criticise public policies," he said.

- *July 2014 - Summary of the Human Rights Council panel discussion on the safety of journalists: Report of the Office of the United Nations High Commissioner for Human Rights*

The Summary noted that: "A recurrent issue raised during the discussion was the question of whether the current legal framework was sufficient for ensuring the safety and protection of journalists and media workers. The issue was looked at in terms of both the physical protection against threats and violence and protection against undue interference, including legal or administrative" (UN HRC: 2014).

Further, the summary noted that the emergence of new forms of journalism (including social networks and blogs) has led to "greater vulnerability of the media, including illegal interference in the personal lives and activities of journalists. Such interference was to be condemned and the independence of the traditional and digital media supported" (UN HRC 2014, p11).

These points are relevant to journalists' right to receive and report information obtained from confidential sources in the public interest, without interference.

According to the Summary, the then UN HRC Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, stated that privacy and anonymity of journalists were also vital elements to ensuring press freedom.

Speakers also noted that: "bloggers, online journalists and citizen journalists played an important role in the promotion of human rights... [and] stated that the protection of journalists should cover all news providers, both professional and non-professional". This is relevant to the issue of the application of legal protection for journalists' sources.

Finally, the meeting heard that national security and anti-terrorism laws should not be used to silence journalists (UN HRC 2014 a p15).

- *2014 UNESCO World Trends in Freedom of Expression and Media Development report*

The threat of surveillance to journalism is underlined in this global report which highlights the role of national security, anti-terrorism and anti-extremism laws as instruments "…used in some cases to limit legitimate debate and to curtail dissenting views in the media, while also underwriting expanded surveillance, which may be seen to violate the right to privacy and to jeopardize freedom of expression" (UNESCO: 2014c).

This report further notes that:

> *National security agencies across a range of countries have gained access to journalists' documents, emails and phone records, as well as to massive stores of data that have the potential to enable tracking of journalists, sources and whistleblowers*

- *July 2014: 'The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights'*

The UN General Assembly mandated this report on protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale (OHCHR: 2014 p1).

The Report found that in the digital era, communications technologies have enhanced the capacity of "Governments, enterprises and individuals to conduct surveillance, interception and data collection".

It also acknowledged that:

> *Concerns have been amplified following revelations in 2013 and 2014 that suggested that, together, the National Security Agency (NSA) in the United States and General Communications Headquarters (GCHQ) in the United Kingdom of Great Britain and Northern Ireland have developed technologies allowing access to much global internet traffic, calling records, individuals' electronic address books and huge volumes of other digital communications content.*

It is evident that the risks posed by these emerging digital dimensions to the preservation of legally enshrined protections for journalists' confidential sources are significant.

The Report quoted the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion, who said that technological advancements mean that States' effectiveness in undertaking surveillance is no longer limited by factors such as scale or the duration of an operation:

> *The State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before. In other words, the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it.* (OHCHR 2014 p3)

The Report also acknowledged that the problem of surveillance is widespread globally: "Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit, rather than an exceptional measure".

Further, there are also flow-on factors affecting third party intermediaries, according to the Report:

> *Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly made use of surveillance of telecommunications networks to target political opposition members and/or political dissidents. There are reports that authorities in some States routinely record all phone calls and retain them for analysis, while the monitoring by host Governments of communications at global events has been reported. Authorities in one State reportedly require all personal computers sold in the country to be equipped with filtering software that may have other surveillance capabilities. Even non-State groups are now reportedly developing sophisticated digital surveillance capabilities. Mass surveillance technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls*.

The Report also stated: "Practices in many States have…revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy" (OHCHR 2014: pp15-16).

There are clear implications for source protection in the context of such unchecked surveillance and data retention.

The risks of 'big data' are also highlighted in the Report: "…a reality of big data is that once data is collected, it can be very difficult to keep anonymous. While there are promising research efforts underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently in use to re-identify seemingly 'anonymous' data. Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy". Furthermore, the Report noted that "…focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy", in part because "big data enables new, non-obvious, unexpectedly powerful uses of data" (OHCHR: 2014 p6).

The issue of metadata collection (e.g. data that indicates patterns of behaviour - such as the number of calls between two individuals and the timing of the calls, rather than the content) is also highly relevant to source protection: "The aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication," (OHCHR: 2014 p7), the Report continued: "The chilling effect on confidential sources, given the risk of profiling and exposure posed by the combination of data retention and the implications of big data analysis, is therefore further exacerbated.

The Report further proposed that: "…Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association" (OHCHR: 2014 p7) It also stated: "…the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime". In other words,

> …*it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.* (OHCHR: 2014 p9).

The Report concluded that there is a pattern of governments increasingly relying on private sector actors to retain data (often in the context of mandatory data retention legislation that is a common feature of surveillance programs) 'just in case'. It stated that such measures are neither 'necessary', nor 'proportionate'.

Citing a European Court of Human Rights ruling, the report declared the onus should be on the State to ensure that any interference with the right to privacy, family, home or correspondence is authorised by laws that "…are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorising, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and provide for effective safeguards against abuse" (OHCHR: 2014, p10). This prompts the question: Should journalists be excluded from mass surveillance? Is this feasible? And how would journalists/journalism be defined for the purpose of considering such exemptions?

As observed in the report, there is an emerging practice of States to outsource surveillance tasks to others. "There is credible information to suggest that some governments have systematically routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes…States have also failed to take effective measures to protect individuals within their jurisdiction against illegal surveillance practices by other States or business entities, in breach of their own human rights obligations" (OHCHR: 2014 p10).

"If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass 'off-shore' at some point) and thus allow them to be collected and retained". The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens in a country, as compared with those of citizens (OHCHR: 2014, p12). The practice of States sharing their intelligence and bypassing limits on surveilling their own citizens themselves has evident implications for journalists, especially foreign correspondents and journalists conducting international investigations.

The role of third party intermediaries is also referenced in this report. "…Given the growing role of third parties, such as Internet service providers, consideration may also need to be given to allowing such parties to participate in the authorisation of surveillance measures affecting their interests, or allowing them to challenge existing measures" (OHCHR: 2014 p13).

This is an important new dimension relevant to journalists' source protection, as there are increasing pressures on third party intermediaries which may have access to journalists' 'private' digital dealings with confidential sources (such as search engines, ISPs, telcos, and social networks) to hand data over to governments and corporations – in the context of either court proceedings or extra-judicial approaches. This process is increasingly formalised. As telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries…The enactment of statutory requirements for companies to make their networks 'wiretap-ready' is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures" (OHCHR p15).

The report also stated: "On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata" (OHCHR: 2014, p14).

- *November 2014: UNESCO International Program for the Development of Communication (IPDC) Council decision*

In 2014, the IPDC's 39 Member-State council welcomed the UNESCO Director-General's Report on the Safety of Journalists and the Danger of Impunity, which states that it uses the term 'journalists' to designate the range of "journalists, media workers and social media producers who generate a significant amount of public-interest journalism". The Council also reaffirmed the importance of condemnations of "the killings of journalists, media workers and social media producers who are engaged in journalistic activities and who are killed or targeted in their line of duty".

- *July 2015: UNESCO study "Keystones for the Internet"*

The finalised UNESCO study, which was informed by preliminary research flowing from 'Protecting Journalism Sources in the Digital Age', proposed to UNESCO's 195 Member States that they: "Recognise the need for enhanced protection of the confidentiality of sources of journalism in the digital age" (UNESCO 2015). This was also contained in the Outcome Document of the "Connecting the Dots: Options for Future Action" conference convened by UNESCO in 3-4 March 2015. (The point was endorsed at the 38th General Conference of UNESCO's Member States in November 2015 as part of the overall options for a comprehensive agenda of UNESCO's approach to Internet issues.) Responses to the survey attached to this study signalled the importance of UN positions on the issue of journalistic source protection.

- *May 2015: UN Office of the High Commissioner for Human Rights (OHCHR) Report on Encryption, Anonymity and the Human Rights Framework by UN Special on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye (Kaye 2015)*

This report from the new Special Rapporteur emphasises the essential roles played by encryption and anonymity. According to Kaye, these defences – working separately or together - create a zone of privacy to protect opinion from outside scrutiny. He noted the particular importance of the role they play in hostile political, social, religious and legal environments. "Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities". With particular relevance to this study, he highlighted the value of anonymity and encryption to journalists seeking to protect their confidential sources and their communications with them. "Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment".

A related issue addressed by Kaye is a trend involving States seeking to combat anonymity tools, such as Tor, proxies and VPNs, by denying access to them. Such moves can directly undermine attempts to protect confidential journalistic sources in the context of digital communications.

Kaye also acknowledged that many States recognise the lawfulness of maintaining the anonymity of journalists' sources. However, he reports that: "States often breach source anonymity in practice, even where it is provided for in law", highlighting the pressures on journalists that undermine these legal provisions – either directly, or progressively.

Another issue the Special Rapporteur also noted is the increasing prevalence and impact of compulsory SIM card registration on confidential communications, including those between journalists and their sources: "Such policies directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest."

Kaye concluded that States should support and promote strong encryption and anonymity, and he specifically recommended strengthened legal and legislative provisions to enable secure journalistic communications. "Legislation and regulations protecting human rights

defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications."

Summary

United Nations actors have been much engaged in debate about the implications of the emerging digital age threats to legal source protection frameworks. They have commissioned research, initiated inquiries and formulated resolutions relevant to the issues at the core of this study, namely the impacts of surveillance, national security/anti-terrorism legislation, data retention, the role of third party intermediaries, and shifts in entitlement to access protections connected to redefinitions of journalism.

5. Regional Instruments of Human Rights Laws and Normative Frameworks

5.1. European institutions

"The recognition of protection of journalistic sources is fairly well established in Europe both at the regional and domestic levels. For the most part, the protections seem to be respected by authorities…and direct demands to [expose] sources seem more the exception than the common practice" (Banisar: 2007). However, as Banisar also noted when he wrote:

> *...There are still significant problems. Many of the national laws are limited in scope, or in the types of journalists that they protect. The protections are being bypassed in many countries by the use of searches of newsrooms and through increasing use of surveillance. There has also been an increase in the use of criminal sanctions against journalists, especially under national security grounds for receiving information from sources.*

Since then, European organisations and law-making bodies have made significant attempts at a regional level to identify the risks posed to source protection in the changing digital environment, and to mitigate these risks.

a. European Court of Human Rights (Ecthr) and European Union Court of Justice Judgements

- *November 2007: European Court of Human Rights (ECtHR) - Tillack v Belgium (20477/05)*

This case, which dates back to 2002, involved a leak investigation targeting an investigative journalist. Investigators seized 16 crates of papers, two boxes of files, two computers, four mobile telephones and a metal cabinet from the journalist's home and workplace with judicial approval. The journalist argued in the case that the judicial authorities were prohibited from taking measures or decisions intended to force journalists or organs of the press to reveal their sources.

The ECtHR found that the reasons cited for the searches were not sufficient to justify the seizure of the journalists' material, noting the quantity of documents and other items seized. Its judgment concluded that the authorities acted disproportionately and breached the journalist's right to freedom of expression enshrined in Article 10 of the European Convention on Human Rights. The Court made the following statement about the importance of source protection in its judgement:

> *… the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution. This applies all the more in the instant case, where the suspicions against the applicant were based on vague, unsubstantiated rumours, as was subsequently confirmed by the fact that he was not charged (par 65)*

- *February 2008: European Court of Human Rights (ECtHR) Guja v. Moldova (14277/04)*

This judgement found in favour of Jacob Guja, the former head of the Press Department of the Moldovan Prosecutor General, who had served as a whistleblower to a newspaper regarding cases of alleged political interference with the justice process, supplying two letters from public officials to journalists. In the course of a 2003 leak investigation that followed publication of stories based on the letters, Guja admitted that he was the source, and was dismissed from his position shortly afterwards. In February 2008 the Court ruled that that Guja acted in good faith as a confidential source and ordered he be reinstated to his position. This was the first such whistleblower case to reach the ECtHR. However, after being briefly reinstated, Guja was once again dismissed. At the time of writing, his case was under review by the CoE's Committee on the Execution of Judgements (Noorlander 2014).

- *December 2009: European Court of Human Rights (ECtHR) Financial Times ltd and others v. The United Kingdom (821/03)*

In 2009, the European Court of Human Rights (ECtHR) ruled that the Financial Times, *The Guardian*, *The Times*, *The Independent* and Reuters were right to protect their sources by rejecting a UK High Court order for them to turn over leaked documents connected to a takeover bid involving a brewing company. The company began action to seize *The Guardian*'s assets. The publishers argued that they were obliged to protect their sources and cited their freedom of expression rights under Article 10 of the European Convention on Human Rights. The ECtHR ultimately ruled that:

> *…the threat of damage [to the company] through future dissemination of confidential information and in obtaining damages for past breaches of confidence were, even if considered cumulatively, insufficient to outweigh the public interest in the protection of journalists' sources…*

- *September 2010: European Court of Human Rights (ECtHR), Grand Chamber Appeal - Sanoma Uitgevers B.V. v The Netherlands*

In a landmark Grand Chamber judgement, the ECtHR declared illegal the seizure by the Dutch police of a journalist's CD of photographs, which identified confidential sources.

The Court had ruled in 2003 that although the seizure could have a 'chilling effect' on press freedom, the police were pursuing a legitimate aim in seizing the CD because it contained relevant information that could lead to the identification of alleged criminals. The publisher subsequently appealed the case to the Grand Chamber and it found that the seizure was not lawful because it breached Article 10 of the European Convention on Human Rights. It also found that independent oversight was lacking in the case, leading to an absence of adequate legal safeguards to ensure an independent assessment as to whether the interest of the criminal investigation overrode the public interest in the protection of journalistic sources (NJCM 2010).

In its judgement, the Grand Chamber stated:

> *The right of journalists to protect their sources is part of the freedom to "receive and impart information and ideas without interference by public authorities" protected by Article 10 of the Convention and serves as one of its important safeguards. It is a cornerstone of freedom of the press, without which sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public-watchdog role of the press*

may be undermined and the ability of the press to provide accurate and reliable information to the public may be adversely affected.

In its conclusion, the Grand Chamber also highlighted that:

…orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on members of the public, who have an interest in receiving information imparted through anonymous sources

It also made specific statements on the importance of independent judicial oversight as a safeguard in processes that lead to access to journalistic communications:

First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body. The requisite review should be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing-over of such material and to prevent unnecessary access to information capable of disclosing the source's identity if it does not.

- ***November 2012: European Court of Human Rights (ECtHR) Telegraaf Media Nederland Landelijke Media b.v. and others v. the Netherlands (Application no. 39315/06)***

The complaint in this case was brought by a Dutch newspaper and two of its journalists. The journalists had been under investigation after publishing stories in De Telegraaf about the circulation of state secrets, in the form of documents from the Netherlands' secret service (AIVD). AIVD lodged a criminal complaint concerning unlawful disclosure of State secrets and an order was sought to force the journalists to hand over documents connected to the relevant stories. Those documents were initially sealed to prevent finger print analysis while legal challenges ensued. The journalists were jailed for three days in 2006, after refusing to answer questions of a judge in a criminal hearing involving three people charged with involvement in leaking the AIVD documents.

Further, according to the ECtHR judgement, the journalists were placed under surveillance by security operatives from the time the leak investigation began. "The present case is characterised precisely by the targeted surveillance of journalists in order to determine from whence they have obtained their information," the judgement reads. The surveillance orders were not the subject of independent oversight or judicial review according to the Court. Importantly, in terms of securing source confidentiality rights in the context of surveillance used against journalistic actors, the court noted the importance of prior independent review of surveillance requests as they apply to journalistic actors. It stated: "Moreover, review post factum, whether by the Supervisory Board, the Committee on the Intelligence and Security Services of the Lower House of Parliament or the National Ombudsman, cannot restore the confidentiality of journalistic sources once it is destroyed."

Ultimately, the Court found that the journalists' rights under both Articles 8 and 10 of the European Convention on Human Rights had been violated: "…the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources".

- *April 2014: European Union Court of Justice judgement (Ireland Data Retention Directive)*

The Court observed, in its judgment declaring the Data Retention Directive invalid, that communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" (*Digital Rights Ireland Ltd C-293/12 v Minister for Communications et al Ireland*, 8 April 2014, Directive 2006/24/EC). This judgement is significant in relation to the role of metadata in identifying confidential sources and the threat posed by data retention to source protection.

- *May 2014 Stichting Ostade Blade v The Netherlands in the ECtHR (Application no. 8406/06)*

In this case, the Court rejected a Dutch magazine's application against a police raid under Article 10 of the European Convention on Human Rights. This judgement demonstrates the narrow circumstances in which source protection laws can be legitimately over-ridden in the public interest.

The police raid has been conducted with a Court-approved warrant for the purpose of obtaining a letter published by the magazine which claimed responsibility for a bomb attack. The Court acknowledged that the magazine's right to "receive and impart information" had been interfered with through the order to hand over the original letter and the subsequent raid when the magazine refused to comply with that order. However, the Court held that the author of the letter was not a "journalistic source," stating that not "*every individual who is used by a journalist for information is a 'source'*". So, in this case, protection was found to extend only to the journalist.

On the question of necessity, the Court noted that the letter was sought as a possible lead towards identifying those suspected of having carried out bomb attacks. Nevertheless, the Court reiterated the importance of the press as "public watchdog" and the importance of ensuring that individuals remain free to disclose to the press information that should properly be accessible to the public.

The question of the source's motive was also at issue in this case. The magazine's informant was not motivated by the desire to provide information which the public were entitled to know, in the view of the Court. According to the judgement: *"his purpose in seeking publicity through the magazine Ravage was to don the veil of anonymity with a view to evading his own criminal accountability."*

b. Council of Europe (COE) Resolutions, Declarations, Statements, Comments, Recommendations, Report and Guidelines

- *September 2007: Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis adopted*

These guidelines (CoE 2007) recommended that Member States adopt Recommendation No. R (2000)7 (CoE 2000) into law and practice. In March 2000, the Council of Europe's Committee of Ministers had adopted that Recommendation on the "right of journalists not to disclose their sources of information". The following principles were appended to Recommendation No. R(2000)7:

- *Principle 1 (Right of non-disclosure of journalists)*

Domestic law and practice in Member States should provide for explicit and clear protection of the right of journalists not to disclose information identifying a source in accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: the Convention) and the principles established herein, which are to be considered as minimum standards for the respect of this right.

- *Principle 2 (Right of non-disclosure of other persons)*

Other persons who, by their professional relations with journalists, acquire knowledge of information identifying a source through the collection, editorial processing or dissemination of this information, should equally be protected under the principles established herein.

- *Principle 3 (Limits to the right of non-disclosure)*

a. *The right of journalists not to disclose information identifying a source must not be subject to other restrictions than those mentioned in Article 10, paragraph 2 of the Convention. In determining whether a legitimate interest in a disclosure falling within the scope of Article 10, paragraph 2 of the Convention outweighs the public interest in not disclosing information identifying a source, competent authorities of member States shall pay particular regard to the importance of the right of non-disclosure and the pre-eminence given to it in the case-law of the European Court of Human Rights, and may only order a disclosure if, subject to paragraph b, there exists an overriding requirement in the public interest and if circumstances are of a sufficiently vital and serious nature.*

b. *The disclosure of information identifying a source should not be deemed necessary unless it can be convincingly established that:*

   i. *reasonable alternative measures to the disclosure do not exist or have been exhausted by the persons or public authorities that seek the disclosure, and*

   ii. *the legitimate interest in the disclosure clearly outweighs the public interest in the non-disclosure, bearing in mind that:*

   – *an overriding requirement of the need for disclosure is proved,*

   – *the circumstances are of a sufficiently vital and serious nature,*

   – *the necessity of the disclosure is identified as responding to a pressing social need, and*

   – *member States enjoy a certain margin of appreciation in assessing this need, but this margin goes hand in hand with the supervision by the European Court of Human Rights.*

c. *The above requirements should be applied at all stages of any proceedings where the right of non-disclosure might be invoked.*

- *Principle 4 (Alternative evidence to journalists' sources)*

In legal proceedings against a journalist on grounds of an alleged infringement of the honour or reputation of a person, authorities should consider, for the purpose of establishing the truth or otherwise of the allegation, all evidence which is available to them under national procedural law and may not require for that purpose the disclosure of information identifying a source by the journalist.

- *Principle 5 (Conditions concerning disclosures)*

a. *The motion or request for initiating any action by competent authorities aimed at the disclosure of information identifying a source should only be introduced by persons or public authorities that have a direct legitimate interest in the disclosure.*

b. *Journalists should be informed by the competent authorities of their right not to disclose information identifying a source as well as of the limits of this right before a disclosure is requested.*

c. *Sanctions against journalists for not disclosing information identifying a source should only be imposed by judicial authorities during court proceedings which allow for a hearing of the journalists concerned in accordance with Article 6 of the Convention.*

d. *Journalists should have the right to have the imposition of a sanction for not disclosing their information identifying a source reviewed by another judicial authority.*

e. *Where journalists respond to a request or order to disclose information identifying a source, the competent authorities should consider applying measures to limit the extent of a disclosure, for example by excluding the public from the disclosure with due respect to Article 6 of the Convention, where relevant, and by themselves respecting the confidentiality of such a disclosure.*

- *Principle 6 (Interception of communication, surveillance and judicial search and seizure)*

a. *The following measures should not be applied if their purpose is to circumvent the right of journalists, under the terms of these principles, not to disclose information identifying a source:*

   i. *interception orders or actions concerning communication or correspondence of journalists or their employers,*

   ii. *surveillance orders or actions concerning journalists, their contacts or their employers, or*

   iii. *search or seizure orders or actions concerning the private or business premises, belongings or correspondence of journalists or their employers or personal data related to their professional work.*

b. *Where information identifying a source has been properly obtained by police or judicial authorities by any of the above actions, although this might not have been the purpose of these actions, measures should be taken to prevent the subsequent use of this information as evidence before courts, unless the disclosure would be justified under Principle 3.*

- *Principle 7 (Protection against self-incrimination)*

The principles established herein shall not in any way limit national laws on the protection against self-incrimination in criminal proceedings, and journalists should, as far as such laws apply, enjoy such protection with regard to the disclosure of information identifying a source.

A question of particular relevance to this study is how such principles might extend to online conduct. The definitions attached to Recommendation (2000)7 include the following detail which addresses this question:

c. *the term "information identifying a source" means, as far as this is likely to lead to the identification of a source:*

   i. *the name and personal data as well as voice and image of a source,*

   ii. *the factual circumstances of acquiring information from a source by a journalist,*

   iii. *the unpublished content of the information provided by a source to a journalist, and*

   iv. *personal data of journalists and their employers related to their professional work.*

In regards to the definition of a journalist, the Recommendation states that the laws should protect "any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication".

The CoE's 2007 guidelines that reference Recommendation R(2000)7 further recommended that:

> *With a view, inter alia, to ensuring their safety, media professionals should not be required by law-enforcement agencies to hand over information or material (for example, notes, photographs, audio and video recordings) gathered in the context of covering crisis situations nor should such material be liable to seizure for use in legal proceedings*.

- ***2010: Report on the protection of journalists' sources from the Council of Europe (CoE) Parliamentary Assembly***

This Report pointed directly to the core issues examined in this study. It stated:

> *"The protection of journalists' sources of information is a basic condition for both the full exercise of journalistic work and the right of the public to be informed on matters of public concern. In a large number of cases, public authorities have forced, or attempted to force, journalists to disclose their sources, despite the clear standards set by the European Court of Human Rights and the Committee of Ministers of the Council of Europe".*

The Report also highlighted the need to limit exceptions to legal source protection provisions. "The disclosure of information identifying a source should therefore be limited to exceptional circumstances where vital public or individual interests are at stake and can be convincingly established". It referenced the emergence of threats to journalistic source protection in the digital age: "The confidentiality of journalists' sources must not be compromised by the increasing technological possibilities for public authorities to control the use by journalists of mobile telecommunication and Internet media".

Further, it recommended that: "Member states which have not passed legislation specifying the right of journalists not to disclose their sources of information should pass such legislation in accordance with the case-law of the European Court of Human Rights and the Committee of Ministers' recommendations".

- ***2011: Council of Europe Human Rights Commission issues discussion paper on Protection of Journalists from Violence (CoE HRC 2011)***

This Report by the CoE Commissioner for Human Rights directly linked journalistic source protection to journalists' safety. "Practical guarantees of nondisclosure of confidential

sources of journalists are also a tool to avoid unnecessary risks of the profession" (CoE HRC 2011).

It also referenced a 1996 European Court of Human Rights judgement [*Goodwin v. the United Kingdom* (27 March 1996)] that "[p]rotection of journalistic sources is one of the basic conditions for press freedom ... Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected". The Court concluded in that case that, in the absence of "an overriding requirement in the public interest", an order to disclose sources would "violate the guarantee of free expression enshrined in Article 10 of the European Convention on Human Rights (ECHR)".

It was this case that led the Council of Europe's Committee of Ministers to adopt Recommendation No. R (2000)7 (See earlier discussion in this section) on the right of journalists not to disclose their sources of information. The CoE discussion paper reaffirmed that the basic protections of confidentiality of journalists' sources were not undercut by security efforts, recalling a declaration (2005) that member states should not undermine protection of sources in the name of fighting terrorism, and noting that "the fight against terrorism does not allow the authorities to circumvent this right by going beyond what is permitted [Article 10 of the ECHR and Recommendation R (2000) 7]" (See explanation of Recommendation R (2000)7 above).

- ***2011: Council of Europe Parliamentary Assembly adopted Recommendation 1950 on the protection of journalists´ sources. (CoE 2011)***

This Recommendation reaffirmed the centrality of source protection to democratic journalistic function:

> *Recalling Committee of Ministers Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information, the Assembly reaffirms that the protection of journalists' sources of information is a basic condition for both the full exercise of journalistic work and the right of the public to be informed on matters of public concern, as expressed by the European Court of Human Rights in its case law under Article 10 of the Convention.*

It also acknowledged the existence of violations of the principles of source protection in Europe. Specifically, this 2011 recommendation noted broad exceptions to source protection in Hungary and called on the Government to amend the law which it described as being:

> *…overly broad and thus may have a severe chilling effect on media freedom. This law sets forth neither the procedural conditions concerning disclosures, nor guarantees for journalists requested to disclose their sources.*

Additionally, this Recommendation required that exceptions to source protection laws be narrowly designed to prevent widespread demands from authorities for source revelation:

> *Public authorities must not demand the disclosure of information identifying a source unless the requirements of Article 10, paragraph 2, of the Convention are met and unless it can be convincingly established that reasonable alternative measures to disclosure do not exist, or have been exhausted, the legitimate interest in the disclosure clearly outweighs the public*

interest in the non-disclosure, and an overriding requirement of the need for disclosure is proved.

The legitimate interest referred to above is specified in Article 10 (freedom of expression) paragraph 2 of the European Convention on Human Rights [1953 1. Assembly debate on 25 January 2011 (4th Sitting) see Doc. 12443, report of the Committee on Culture, Science and Education). Text adopted by the Assembly on 25 January 2011 (4th Sitting)]. This invokes national security rather broadly, which is seen by some observers to undercut legal frameworks for source protection globally. However, the CoE Recommendation does nevertheless did add stronger limits to any exceptions to source confidentiality protection to correspond to:

> … *exceptional circumstances where vital public or individual interests are at stake and can be convincingly established. The competent authorities, requesting exceptionally the disclosure of a source, must specify the reasons why such vital interest outweighs the interest in the non-disclosure and whether alternative measures have been exhausted, such as other evidence. If sources are protected against any disclosure under national law, their disclosure must not be requested*.

The Recommendation also pointed to the importance of confidential sources within the police and judiciary, and the right of journalists not to disclose them. "Where such provision of information to journalists was illegal, police and judicial authorities must pursue internal investigations instead of asking journalists to disclose their sources". The problem of data retention in connection with source protection is also referenced in the Recommendation:

> Referring to the European Union's Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, the Assembly insists on the need to ensure that legal provisions enacted by member states when transposing this directive are consistent with the right of journalists not to disclose their sources under Article 10 of the Convention and with the right to privacy under Article 8 of the Convention.

Importantly, the Recommendation highlights the importance of applying the principles of confidential information sharing to third party intermediaries:

> *In so far as Article 10 of the Convention protects the right of the public to be informed on matters of public concern, anyone who has knowledge or information about such matters should be able to either post it confidentially on third-party media, including Internet networks, or submit it confidentially to journalists.*

This is relevant to the emerging threat of pressure applied to third party intermediaries to hand over data to authorities or litigants, thereby circumventing source protection laws.

According to the Recommendation:

> *The Assembly reaffirms that the confidentiality of journalists' sources must not be compromised by the increasing technological possibilities for public authorities to control the use by journalists of mobile telecommunication and Internet media. The interception of correspondence, surveillance of journalists or search and seizure of information must not circumvent the protection of journalists' sources. Internet service providers and telecommunication companies should not be obliged to disclose information which may lead to the identification of journalists' sources in violation of Article 10 of the Convention.*

The Recommendation also indicated the need to extend source protections to non-traditional media platforms in line with changes in professional practice, publishing and distribution modes, the role of social media, and participatory audiences and sources:

> *In the same manner as the media landscape has changed through technological convergence, the professional profile of journalists has changed over the last decade. Modern media rely increasingly on mobile and Internet-based communication services. They use information and images originating from non-journalists to a larger extent. Non-journalists also publish their own or third-party information and images on their own or third-party Internet media, accessible to a wide and often undefined audience. Under these circumstances, it is necessary to clarify the application of the right of journalists not to disclose their sources of information.*

Nevertheless, the Recommendation took the position that bloggers and social media actors are not journalists and therefore should not be able to claim access to source protection laws:

> *The right of journalists not to disclose their sources of information is a professional privilege, intended to encourage sources to provide journalists with important information which they would not give without a commitment to confidentiality. The same relationship of trust does not exist with regard to non-journalists, such as individuals with their own website or web blog. Therefore, non-journalists cannot benefit from the right of journalists not to reveal their sources.*

This conflation of 'journalism' with 'journalists' could, in effect, exclude a significant number of important journalistic actors – such as academic or legal bloggers, activists with human rights organisations who use social media as platforms to share information imparted confidentially in the public interest, journalism educators and their students.

On a different issue, the synergies between whistleblower protections and legal frameworks designed to protect journalists from being compelled to reveal their sources were also recognised in the Recommendation:

> *With regard to the right of every person to disclose confidentially to the media, or by other means, information about unlawful acts and other wrongdoings of public concern, the Assembly recalls its Resolution 1729 (2010) and Recommendation 1916 (2010) on the protection of "whistle-blowers" and reaffirms that member states should review legislation in this respect to ensure consistency of domestic rules with the European standards enshrined in these texts.*

Finally, the Assembly recommended that the Committee of Ministers call on all their Member States to:

- Legislate for source protection
- Review their national laws on surveillance, anti-terrorism, data retention, and access to telecommunications records
- Co-operate with journalists' and media freedom organisations to produce guidelines for prosecutors and police officers and training materials for judges on the right of journalists not to disclose their sources

- Develop guidelines for public authorities and private service providers concerning the protection of the confidentiality of journalists' sources in the context of the interception or disclosure of computer data and traffic data of computer network

- ***2014 Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors adopted:***

This Declaration stated:

> *A favourable environment for public debate requires States to refrain from judicial intimidation by restricting the right of individuals to disclose information of public interest through arbitrary or disproportionate application of the law, in particular the criminal law provisions relating to defamation, national security or terrorism. The arbitrary use of laws creates a chilling effect on the exercise of the right to impart information and ideas, and leads to self-censorship.*

Furthermore, it declared that "…prompt and free access to information as the general rule and strong protection of journalists' sources are essential for the proper exercise of journalism, in particular in respect of investigative journalism".

The Committee of Ministers also directly addressed the implications of mass surveillance for source protection: "Surveillance of journalists and other media actors, and the tracking of their online activities, can endanger the legitimate exercise of freedom of expression if carried out without the necessary safeguards, and it can even threaten the safety of the persons concerned. It can also undermine the protection of journalists' sources".

The Committee also agreed to consider further measures regarding the alignment of laws and practices concerning defamation, anti-terrorism and protection of journalists' sources with the European Convention on Human Rights.

- ***January 2015: Council of Europe Committee on Legal Affairs and Human Rights, Report on Mass Surveillance/Resolution and recommendation***

This Report, prepared by Rapporteur Pieter Omtzigt, on the impact of mass surveillance on human rights, addressed the implications for journalistic source protection in the context of freedom of expression and access to information. He stated:

> *When authors, journalists or civil society activists are reluctant to write, speak, or pursue research about certain subjects (e.g. the Middle East, criticisms of the government post-9/11, the Occupy movement, military affairs, etc.), or to communicate with sources or friends abroad for fear that they will endanger their counterparts by so doing, this does not only affect their freedom of speech, but also everyone else's freedom of information. (COE, Omtzigt 2015 p25)*

The Report also connected the detainment of *Guardian* journalist Glen Greenwald's partner to the impact of surveillance. Greenwald was Snowden's original confidante and court documents reveal that both Greenwald and his partner were under surveillance due to suspicion that they were transporting data associated with Snowden's files. According to the Report, the Brazilian citizen had his mobile phone, laptop, DVDs and other items seized.

- ***January 2015: CoE Resolution and Recommendation on mass surveillance***

The Council of Europe Committee on Legal Affairs and Human Rights unanimously adopted a Resolution, and a Recommendation, based on the Report discussed above, on January 26th 2015. The Resolution included the following statements:

> *The Parliamentary Assembly is deeply concerned about mass surveillance practices disclosed since June 2013 by journalists to whom a former US national security insider, Mr. Edward Snowden, had entrusted a large amount of top secret data establishing the existence of mass surveillance and large-scale intrusion practices hitherto unknown to the general public and even to most political decision-makers.*

In the context of this concern, the Resolution makes the following additional points:

- *The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 European Convention on Human Rights (ECHR)), freedom of information and expression. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law.*
- *It is also worried by the collection of massive amounts of personal data by private businesses and the risk that these data may be accessed and used for unlawful purposes by state or non-state actors.*
- *The Assembly is also deeply worried by the extensive use of secret laws, secret courts and secret interpretations of such laws, which are very poorly scrutinized.*

Relevantly, the associated Recommendation proposed by the Committee invited the CoE Council of Ministers to consider:

- *Addressing a recommendation to Member States on ensuring the protection of privacy in the digital age and internet safety in the light of the threats posed by the newly disclosed mass surveillance techniques*

c. Council of the European Union Resolutions, Declarations, Reports and Guidelines

- *May 2014: Council of the European Union - "EU Human Rights Guidelines on Freedom of Expression: Online and Offline"*

These guidelines included the following pertinent statements:

> *States should protect by law the right of journalists not to disclose their sources in order to ensure that journalists can report on matters in the public interest without their sources fearing retribution. All governments must allow journalists to work in a free and enabling environment in safety and security, without the fear of censorship or restraint.*

The EU will "support the adoption of legislation that provides adequate protection for whistle-blowers and support reforms to give legal protection to journalists' right of non-disclosure of sources".

5.2 The Americas

Regarding Latin America, Banisar (2007) wrote:

> *There are also important declarations from the Organisation of American States (OAS). Few journalists are ever required to testify on the identity of their sources. However direct demands for sources still occur regularly in many countries, requiring journalists to seek legal recourse in courts. There are also problems with searches of newsrooms and journalists' homes, surveillance and the use of national security laws.* (Banisar, 2007: 81)

In 1997, the Hemisphere Conference on Free Speech staged in Mexico City adopted the Chapultepec Declaration. Principle 3 states:

> *No journalist may be forced to reveal his or her sources of information. (Chapultepec Declaration 1997)*

Building on the Chapultepec Declaration, in 2000 the Inter-American Commission on Human Rights (IACHR) approved the Declaration of Principles on Freedom of Expression as a guidance document for interpreting Article 13 of the Inter American Convention of Human Rights. Article 8 of the Declaration states:

> *Every social communicator has the right to keep his/her source of information, notes, personal and professional archives confidential*. (Organisation of American States 2000)

The application of the term 'social communicator' has resonance with the 'who is a journalist?' debate in reference to shield laws. There are noteworthy developments with regards to the status of the above regional instruments since 2007:

- ***Guatemala 2013***: (The then) President Otto Pérez Molina expressed interest in signing the Declaration of Chapultepec, however he later suspended the signing.
- ***Venezuela 2013***: announced its withdrawal from the Inter-American Commission on Human Rights (IACHR) and the Inter-American Court of Human Rights.

In 2013, the Inter American Commission on Human Rights report *Violence Against Journalists and Media Workers: Inter American Standards and National Practices on Prevention, Protection and Prosecution of Perpetrators* by the Office of the Special Rapporteur for Freedom of Expression provided the following definition of journalists relevant to debates about source protection entitlement:

> *…journalists are those individuals who observe and describe events, document and analyse events, statements, policies, and any propositions that can affect society, with the purpose of systematizing such information and gathering facts and analyses to inform sectors of society or society as a whole. Such a definition of journalists includes all media workers and support staff, as well as community media workers and so-called "citizen journalists" when they momentarily play this role. Such definition also includes persons who might be using new communications media as a tool to reach the public, as well as opinion makers who are targeted for the exercise of their right to freedom of expression.* (Botero 2013 p2)

5.3. Africa

Article 9 of the African Charter of Human Rights gives every person the right to receive information and express and disseminate opinions (Banisar, 2007:20). The 2002 Declaration of Principles on Freedom of Expression in Africa, released by the African Commission on Human and People's Rights, provided guidelines for member states of the AU on protection of sources:

XV Protection of Sources and other journalistic material

Media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except in accordance with the following principles:

- *The identity of the source is necessary for the investigation or prosecution of a serious crime, or the defence of a person accused of a criminal offence;*
- *The information or similar information leading to the same result cannot be obtained elsewhere;*
- *The public interest in disclosure outweighs the harm to freedom of expression;*
- *And disclosure has been ordered by a court, after a full hearing.*

Noteworthy developments since 2007:

- April 2013 - Model Law on Access to Information in Africa by the Special Rapporteur on Freedom of Expression and Access to Information at the African Commission on Human and People's Rights was circulated.

An information officer may refuse a request if the information: "(c) Consists of confidential communication between a journalist and her or his source".

- May 2015 - East African Court of Justice (EAJC) judgement on Burundi Press Law (Burundian journalists' union v the Attorney General of the Republic of Burundi, Reference No.7 of 2013)

In this judgement, the EAJC ruled Articles 19 & 20 of Burundi's 2013 Press Law violated democratic principles and should be repealed.

Article 20 of the 2013 Press law obligates journalists to "reveal their sources of information before the competent authorities in situations where the information relates to State security, public order, defence secrets and the moral and physical integrity of one or more persons". However, the judges upheld the challenge originally brought by the Burundi Journalists Union, referring to the need for proportionality and necessity with regard to exceptions to source protection – even in cases of national security. They cited the Goodwin vs. UK judgment which states:

> *Protection of journalistic sources is one of the basic conditions for press freedom .... Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected".*

The judges in the Burundi case explained their position thus:

> *…because whereas the four issues named are important in any democratic state, the way of dealing with State secrets is by enacting other laws to deal with the issue and not by forcing journalists to disclose their confidential sources… . As for the issue of moral and physical integrity of any person, the obligation to disclose a source is unreasonable and privacy laws elsewhere can be used to deal with the matter. There are in any event other less restrictive ways of dealing with these issues.*

They concluded: "We have no hesitation in holding that Article 20 does not meet the expectations of democracy and is in violation of Articles 6(d) and 7(2) of the Treaty"

5.4 Asia and the Pacific

The Association of Southeast Asian Nations (ASEAN) adopted a Human Rights Declaration in November 2012 with general provisions for freedom of expression and privacy (ASEAN 2012). Reservations have, however, been voiced regarding the wording of provisions on human rights and fundamental freedoms in relation to political, economic and cultural systems and the Declaration's provisions on "balancing" rights with individual duties as well as an absence of reference that legitimate restrictions of rights must be provided by law and conform to strict tests of necessity and proportionality (UN 2012; OHCHR (UN) 2012a; OHCHR (UN) 2012b).

5.5. Inter-regional institutions

a. Organisation for Security and Co-operation in Europe (OSCE)

The OSCE Representative on Freedom of the Media (RFOM) regularly issues statements and comments regarding breaches and threats to legal source protection frameworks. Several of these statements are referenced in the Regional Overviews section below, in the context of specific incidents. Additionally, the following recommendations are relevant:

- *June 2011 Organisation for Security and Cooperation in Europe (OSCE) – Representative on Freedom of the Media: Vilnius Recommendations on Safety of Journalists (OSCE 2011)*

This set of recommendations included the following point relevant to source protection in connection with journalism safety: "Encourage legislators to increase safe working conditions for journalists by creating legislation that fosters media freedoms, including guarantees of free access to information, protection of confidential sources, and decriminalising journalistic activities."

b. The Organisation for Economic Co-operation and Development (OECD)

- *April 2013 draft report published: "CleanGovBiz Integrity in Practice, Investigative Media" (OECD 2013)*

This Report asked the questions: "Are journalists guaranteed to keep their information sources private? If so, how is this ensured?" It acknowledged that: "It can be dangerous for members of the public to provide journalists with information, especially if that information denounces serious misbehaviour or pertains to corruption. That is why people often only agree to speak up anonymously. The journalists can then use the information but will not make the name of this source public."

The Report argued that forcing a journalist to reveal a source in such cases would be a short sighted approach in many cases: "…once a corruption case has been brought to light by a journalist, law enforcement has an incentive to discover the anonymous source(s). While

the source might indeed be valuable for the case in question either by providing additional information or through being a witness in court forcing the journalist to reveal the source would often be short-sighted."

The Report, which also cited the CoE Committee of Ministers' Recommendation R(2000)7, pointed out the broader risks of unmasking journalists' confidential sources:

> *With chances being high that anonymity might be lifted, less people will risk disclosing information to journalists in the future. Revealing sources limits the ability of people to impart information and reduces the ability of the public to receive information, both of which are rights granted by Article 19 the Universal Declaration of Human Rights. Journalistic sources should therefore be protected by law.*

Further, the Report stipulated that such protection "should not only include the journalists' contact persons but also their own workspace and research". And it argued that: "Exceptions should only be granted by a judge and only for key witnesses and serious crimes," highlighting the importance of clearly specifying restrictions, "so that journalists can reliably inform their potential sources about the risks involved".

5.6. Regional Instruments of Human Rights Law - conclusion

Significant progress has been made in the European regional context with regards to addressing the emerging threats to legal source protection environments in the digital era. In Latin America and Africa, there is some recognition of the extent of gaps in addressing legislative and normative environments regarding source protection in digital contexts.

6. Overviews by UNESCO Region

Ultimately, developments with actual or potential relevance to legal and regulatory environments regarding protections for journalists' sources were recorded in 84 out of the 121 countries (69%) studied for this report, during the period 2007-2015. These developments were identified through a process of studying 121 UNESCO member States in accordance with the methodology outlined earlier in this Study. They have been analysed with a particular emphasis on digital dimensions and the key identified themes of:

a. The overriding or 'trumping effect' of National Security/Anti-terrorism legislation

b. The potential of surveillance (mass and targeted) in undercutting legal protections

c. The potential of third party intermediaries and data retention

d. Changes affecting entitlement to protection – Who is a journalist?/What is journalism?

e. Other digital dimensions (e.g. risk of confiscation of electronic equipment which may include confidential source information)

f. Anonymity issues

g. Other dimensions

This study has not conducted an in-depth assessment of national security/anti-terrorism laws in every case. Therefore, it should not be inferred that every such law automatically translates into a threat to source protection. The problem arises when such laws may expressly override legal source protection frameworks or are used to justify access to journalistic communications where such access is not independently assessed as to whether it is 'necessary or proportionate', and where definitions of national security are overly broad and can allow for abuse.

This study further does not presume that all changes affecting surveillance, data retention and third parties necessarily impact on the confidentiality of journalistic sources, but that these may have significance for strengthening or weakening such confidentiality. Likewise, with the legal definitions of journalists and journalism. Therefore, the references below to any developments in these areas are primarily to draw attention to issues that in principle can have a bearing on confidentiality. Accordingly, States and other actors seeking to protect such confidentiality are alerted to the range of issues within the ecosystem of journalism and its sources.

It is also necessary to note that factors such as confiscation of digital devices and issues of anonymity in a society are signalled below on the same basis, i.e. without prejudging the specific cases mentioned. Instead, there are examples of developments uncovered by this research that point to the kind of changes that may be of direct or indirect relevance to source protection. The research does not go into issues of the legality of confiscation of journalists' equipment in any instance listed below, but rather signals these instances on the basis that any confiscation per se may have implications for digital confidentiality issues concerning journalists' sources.

Further research into each country studied is recommended in order to assess the full impact of all issues pertaining to source protection in each case. Under the constraints of time and budget, it was not possible to evaluate the extent to which any change registered

was indeed of relevance to source protection. The reported information is therefore not necessarily representative of trends in any society.

Overall, the information below does not purport to assess whether a particular given development was positive, negative or ambiguous for source confidentiality protection, whether in practice or in potential. Nevertheless, the information provided is a pointer to the range of intersecting developments within UNESCO regions, which developments have bearing for source protection issues in the digital age. The data is thus indicative of potential issues, and does not make any claim to be a comprehensive assessment.

The countries studied in this report have been divided into UNESCO regional groups, as follows:

i. Africa

ii. Arab States

iii. Asia and the Pacific

iv. Europe and North America

v. Latin America and The Caribbean.

6.1. Africa

"In Africa, there exists a relatively strong recognition of the right of journalists to protect their sources, at national, sub-regional as well as continental levels. However, and by and large, this recognition has not yet resulted in a critical mass of legal provisions" (Banisar, 2007: 53).

This study has identified relevant developments with direct or potential relevance to source protection trends between 2007-2015 in 18 out of 32 countries[11] (56%) that have been examined in the Africa region.

African countries where developments have been noted since 2007:

- Angola
- Botswana
- Burundi
- Cameroon
- Côte d'Ivoire
- Ethiopia
- Gambia
- Kenya
- Lesotho

11 South Sudan is excluded from this study on methodological grounds . But it is recommended for inclusion in future research

- Mauritius
- Niger
- Nigeria
- Rwanda
- Sierra Leone
- Somalia
- South Africa
- Uganda
- Zimbabwe

In 2007, Banisar identified the source protection issues in Africa as follows:

> *In the lion's share of African countries, there is no legal protection of sources whatsoever. In many of the countries that fall under this category, journalists have been subject to criminal and civil sanctions, harassment and torture to force them to reveal their sources. In a few cases, courts have ruled in favour of journalists [who are] being prosecuted by governments for refusing to name sources. Yet this jurisprudence, however positive, has not necessarily led to protection laws being put in place. …Overall, even where national protections are strong on paper, the tendency in practice is for these laws to be flouted – often by security and intelligence services who intimidate journalists through raiding of newsrooms and surveillance.* (Banisar 2007: 53)

In 2015, source protection laws in Africa remain limited. The data collected for this study show that legal developments affecting source confidentiality and its protection in Africa over the past eight years were largely non-digital. As elaborated below, since 2007, Kenya and Niger have introduced a form of legal protection for journalists' sources, while there is a new constitution that affects source protection in Angola. However, in several States, legal source protection frameworks can be seen to have been potentially at risk of erosion by moves to provide broad exclusions to a journalist's right to protect their sources from disclosure on 'national security' grounds, and the criminalisation of breaches. Meanwhile, allegations of mass surveillance emerged as a notable theme in some countries.

a. National security/Anti-terrorism impacts

The themes of national security and mass surveillance are surfacing across Africa. ARTICLE 19's East Africa representative Henry Maina told this Study's researchers there have been cases in multiple countries where journalists have been compelled to disclose their sources in cases linked to terrorism charges (Maina 2015).

In South Africa, the Protection of State Information bill was passed in 2013 after much debate about the definition of national security and whether there should be limited public interest exception (which could apply to cases of source confidentiality). At the time of writing, the bill had not been signed into law by the President (Freedom House (j) 2014; RDM Newswire 2015; PMG).

In Burundi, security-based exceptions to legal protections for journalists' sources (enshrined in a 2003 Press Act) were introduced during the period. A new Press Law promulgated in June 2013 guaranteed journalistic source protection (Burundi Press Law 2013, Article 16). At the same time, this is also restricted under Article 20 of the legislation, which allowed broad exemptions. Article 20 stated that media are required to provide, before the competent courts, the information revealing the source in one of the four following cases:

1. Information concerning state security offenses;
2. Information concerning offenses relating to public order;
3. Information concerning offenses relating to defence secrets;
4. Information concerning offenses relating to the physical and moral integrity of a person or persons

Under the Act, the National Communications Council (NCC) had the authority to issue warnings to journalists who failed to comply, and three NCC warnings could lead to suspension or deregistration. However, there were two significant developments regarding this law. In March 2015, the National Assembly repealed elements of the act, including the exceptions to source protection guarantees (Rhodes 2015). The Burundi Senate was considering these amendments at the time of writing. Secondly, the East African Court of Justice (see also regional instruments section above) ruled that sections of the 2013 Press Law (including Article 20, which stipulated exceptions to the journalists' privilege) contravened principles of democracy and accountability in the constitution of the East African Community (Burundian journalists' union v the Attorney General of the Republic of Burundi, Reference No.7 of 2013). At the time of writing it was not possible to establish how the Burundi Government had responded to the judgement.

In Kenya, after a terrorist attack in 2013, journalists were asked to reveal the source of leaked CCTV footage which appeared to show looting soldiers. The request was later withdrawn and an investigation into the soldiers' behaviour led to the sacking and imprisonment of those found guilty of looting (ARTICLE 19 2013a; Zadock, A 2013; Saul, H 2013; BBC 2013b).

In Cameroon, two journalists (working for two separate newspapers) were barred by a military tribunal from practicing journalism, and banned from leaving the country on national security grounds in 2014, after they refused to hand over reporting materials from a confidential source. Further hearings were pending at the time of writing and the National Communications Council (NCC) was investigating the actions (Ezieh 2014).

b. Mass surveillance and targeted surveillance

Between 2009 and 2014, three African countries introduced laws authorising surveillance, without exemptions for journalistic communications. (The Security Laws (amendment) Act 2014, Kenya; The Information and Communications Act Section 2009, 138, Gambia; Anti-terrorism Proclamation No.652/2009, Ethiopia).

In Uganda, following a terrorist attack in the capital Kampala in 2010, *The Regulation of Interception of Communications Act 2010* was passed by the Ugandan Government to reinforce the provisions in the *Anti-Terrorism Act No.14 of 2002* legislation. The two pieces of legislation operate in tandem, allowing the authorities to intercept and monitor letters, packages, bank details, calls, faxes, emails and other communications, as well as monitoring

meetings of any groups of persons following consent from a high court judge (s19 Anti-Terrorism Act No. 14 2002; CIPESA 2014). Under Section 5, subsection (1)(c)(d)&(e) a magistrate will grant a warrant for a lawful intercept if there is a terrorist threat (Uganda, 2002; CIPESA 2014).

Spyware attacks in 2014 and 2015 on the US-based Ethiopian Satellite Television Service (ESAT), were reported by the Citizen Lab at Canada's Munk School of Global Affairs at the University of Toronto, potentially putting source confidentiality as risk (Marczak et al 2015; CPJ 2015c). Reports on monitoring of the cell phones of two South African journalists surfaced between 2010 and 2014 (Duncan 2014; IOL 2015; Right to Know 2014).

c. Data retention and third party intermediaries

This is an issue receiving attention in Uganda, where in December 2014, the National Information Technology Authority of Uganda, together with the Ministry of Information and Communications Technology and the Ministry of Justice and Constitutional Affairs, released the draft of a Data Protection and Privacy Bill for public consultation (Draft of 20th August 2014, The Data Protection and Privacy Bill of 2014). The proposed law aimed to safeguard the rights of individuals whose data is collected by government and both public and private institutions (NITA 2014; OpenNet Africa 2015; Monitor 2015). The bill stipulated that personal data may only be collected and processed with the prior consent of the data's subject, unless an exemption is satisfied, such as for the purposes of national security (FADV 2014). The bill would impose notification requirements of the data's subject, which required the individual to be notified prior to data collection, including the nature of the data, the purpose for which the data is required, right to access data, right to rectify the data and whether the data required is discretionary or mandatory (section 9(1) (CIPESA 2014). It would also impose penalties on 'data controllers' who knowingly or recklessly obtain or disclose personal data (FADV 2014).

Additionally, s79 of the Ugandan Communications Commission Act 2013 stated that any operator of a communications service or system who 'unlawfully intercepts any communication' between persons using that service is liable to imprisonment or a fine (UCC 2013). These propositions for transparency and accountability measures regarding data collection and handover could aid journalists in their efforts to protect their sources. At the same time, Section 4(2) of the legislation, which states that personal data may be collected or processed where the collection or processing is necessary for 'national security' is broad and could be open to misinterpretation.

In Niger, the 2005 Computer Security and Critical Information Infrastructure Protection Bill mentioned in Banisar (2007: 63), which mandated ISPs to provide data to law enforcement agencies, failed to pass in 2011 (This Day Live, 2011).

The Angolan government introduced a cybercrime bill in 2011 that would have expanded the authorities' ability to seize citizens' personal data, without exceptions that could be relevant to journalistic communications. The bill won initial approval in the parliament but the Government later withdrew it.

d. Entitlement to protection: Who is a journalist/What is journalism?

The 2013 Press Law in Burundi introduced new professional requirements for journalists, including: holding a Bachelor of Journalism, or any bachelors degree accompanied by completion of a training course or two years practical journalism experience. They are also required to have journalism as a "regular and paid principal activity" and to exercise the profession in "one or more newspaper companies" (Burundi Press Law 2013) This definition of a professional journalist could limit the range of journalistic actors claiming source protection.

In Uganda, new source protection provisions introduced under Section 38 of the amended *Press and Journalists Act* (2010) (See discussion above) required a journalist to be registered in order to enjoy source protection. In Somalia, a draft media bill required defining the term 'journalist' to include Somali nationality, journalism knowledge, and three years experience in the media industry (Article 24, draft media bill, NUSOJ, 2014). The Code of Conduct for the Practice of Journalism in Kenya's Media Council Act 2013 is restricted to: "a journalist, media practitioner, foreign journalist or media enterprise".

e. Other digital dimensions

There have been a number of reported incidents of journalists' devices being taken, something that as noted earlier, may have the potential for exposure of confidential sources. For example, in Uganda, a journalist's laptop and mobile phone were confiscated during an investigation (CIPESA 2014). In Angola, computers at a newspaper were confiscated in 2012 (CPJ 2012b; Freedom House 2013c). In Botswana, in 2014 the editor of *Sunday Standard* had his computer taken by police (ENCA 2014; CPJ 2014b; Mail & Guardian 2014). The examples here, like those below, are not provided with the presumption that confidential data was unduly exposed in these cases but that such exposure was a risk.

f. Anonymity issues

None were recorded in this region by the researchers during the period under study.

g. Other dimensions

In Zimbabwe, a new Constitution adopted in 2013 contains specific provisions for the protection and confidentiality of journalists' sources. Section 61.2 of the Constitution states that "Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information" (The Constitution of Zimbabwe Amendment (No. 20) Act 2003). Calls have also been made to align media and access to information laws, provisions for the interception and monitoring of communications contained in the 2007 Interception of Communications Act, and provisions for criminal defamation contained in the Crimial Law (Codification and Reform Act) with the new Constitution (New Zimbabwe 2013).

In South Africa, there have been calls to amend apartheid-era legislation such as Section 205 of the Criminal Procedure Act, under which journalists have been subpoenaed to reveal their sources. In 2010, two journalists were prosecuted under this law to reveal the identities of sources (Dibetle 2010). The case was adjourned to enable mediation between

the TV network, the South African National Editors Forum (SANEF) and the police (Malumo 2010). SANEF argued that authorities in the case had not followed a Memorandum of Understanding (MOU) brokered by the body in 1999, which outlined a process to follow in the event of authorities seeking confidential source information from journalists (SANEF 2010a. See also SANEF 2010b). One of the journalists subpoenaed told this study's researchers that they were ultimately able to protect the identity of their sources and that the MOU is still in place (Said 2015)

While South Africa has not introduced explicit protection for journalists' sources, partly in response to journalists' concerns about the risk of legislating obligations, a landmark ruling in 2012 (Bosasa Operation (Pty) Ltd v Basson and Another 09/29700) protected the confidentiality of sources relied on in a *Mail and Guardian* article (Global Journalist 2012.) The South African Constitutional Court refused to hear an appeal against the judgement in 2013, so the ruling stands (Holmes 2013, SANEF 2012).

In May 2013, police received a warrant to search Ugandan newpapers *The Daily Monitor* and *The Red Pepper* in regard to the source of a leaked letter underpinning a story (HRW 2013b; BBC 2013a; CPJ 2013). Also in Uganda, *The Press and Journalist Act* was amended in 2010 and now protects a journalist from revealing the identity of their confidential sources, unless s/he has the consent of the person who gave him/her the information, or on an order of a court law (IFEX 2010).

In Burundi in 2014, two journalists from two independent radio stations were asked to reveal their sources in terms of a summons under the 2013 Media Law. The Law contains provisions for disclosure where reporting is found to jeopardize moral integrity (Rhodes 2014; Hakizimana 2014). In a separate case, in January 2015, Burundian authorities charged, and imprisoned for a period, the director of Radio Publique Africaine, in partial connection with the confidentiality of a source (CPJ 2015a; RSF 2015e; HRW 2015a).

Rwanda introduced a new media law in 2013. The law entitles courts to compel journalists to reveal their sources in any legal proceedings, and not necessarily as a last resort (ARTICLE 19 2013b).

In Kenya, there now exists qualified protection of journalists' sources. Kenya's Media Council Act 2013 (No. 46 of 2013) states that journalists shall use identifiable sources wherever possible, and provides that: "Confidential sources shall be used only when it is clearly in the public interest to gather or convey important information, or when a person providing information might be harmed" (Section 45). It further states: "Unnamed sources shall not be used unless the pursuit of the truth will best be served by not disclosing the source, who shall be known by the editor and reporter" (Odera 2014).

In Niger in 2010, a clause was added to the 1999 Press Ordinance stating that: "the professional journalist cannot be forced to divulge their source of information" (Ordinance No. 2010-035).

In Lesotho, in 2009 the Law Reform Commission was tasked by the minister of communications to review the media regulatory landscape, including the confidentiality of sources (Limpitlaw 2012). At the time of writing, no further developments had taken place.

In Mauritius, the *Media Law and Ethics in Mauritius* preliminary report (2013) by Geoffrey Robertson QC (commissioned by the Prime Minister of Mauritius) recommended a new statutory provision: "No court may require a person to disclose, nor is any person guilty of

contempt for refusing to disclose, the source of information contained in a publication for which he is responsible, unless it is clearly established that such disclosure is essential in the interests of justice" (Government Programme 2010-2015). Additionally, it stated, "Every press code requires, as an ethical rule, that a journalist must protect his or her sources. Without such protection, many sources would not come forward to provide newsworthy information they would 'dry up', as would the supply of news" (Robertson 2013).

In Sierra Leone, when Liberia's ex-President Charles Taylor was being tried by the Special Court for Sierra Leone for crimes against humanity and war crimes, an attempt was made to get a journalist to reveal his source during the trial. However, the presiding judge dismissed the request (Simon 2009).

In Côte d'Ivoire, the Code of Ethics for Ivorian Journalists (2012) states that journalists have the right to protect their sources (Cote d'Ivoire Ministry of Communications, 2012).

In Somalia, under media laws introduced in 2007, a media house must record and keep the voice of a 'confidential source' to disclose before a court (Article 25, subsection 7).

There are no source protection laws covering journalistic actors in Nigeria, according to Toyosi Ogunseye, Editor, The Sunday Punch, interviewed for this study in 2014. Two journalists were detained in 2013 after refusing to reveal the source of a leaked document (Balev 2013).

Regional Conclusion

Many of the developments above, which cover a mix of potential implications for the protection of source confidentiality, have relevance to both digital and non-digital issues. However, there is not a lot of attention in the region that has been given to issues of whether to restrict or protect source confidentiality in the purely digital space – possibly in part because of the relatively low level of access to digital communications in the research period. As more users are able to regularly contribute to and access online news content, this may change. Meanwhile, over the period 2007-2015, 18 out of 32 countries examined did see various developments pertaining to source protection laws, across a number of relevant considerations set out above.

6.2. Arab States

The methodology applied to this study, based on updating the countries covered in the 2007 Privacy International report means that there has not been research on a number of Arab States that have undergone dramatic transition since 2007. However, through this study's research process, the author nevertheless noted specific developments in Tunisia[12], Jordan, Kuwait, Palestine, Iraq, Bahrain, Lebanon, and Yemen. It is recommended that additional research be undertaken in each of these countries in the future.

12 Tunisia was not mentioned in the Banisar report and so the methodology applied to this study disqualifies it from examination. But it is noteworthy that the country introduced Decree-Law 115, article 11 of which introduced protections for journalists' sources, as well as "any person involved in the preparation of news and information" (http://en.rsf.org/IMG/pdf/120214_observations_rsf_code_de_la_presse_gb_-_neooffice_writer.pdf) There are a number of exceptions to this law: where there is an investigation by public authorities to identify sources; a request for a journalist to disclose their sources; reasons from national or state security; dangers to third parties. (ibid). A breach of article 11 by an individual is liable to a year's imprisonment and a fine of 120 dinars (article 14 ibid).

There were six countries in this region out of seven (86%) from the study data set where developments occurred between 2007-2015:

- Algeria
- Egypt
- Mauritania
- Morocco
- Sudan[13]
- Syrian Arab Republic (the)

Emerging themes in this region include the impact of national security legislation, mass surveillance, debate on what constitutes a journalist, as well as non-digital issues.

Rawda Ahmed from the Arabic Network for Human Rights commented on the situation in the Arab States to this Study's researchers: "The laws in most of the Arab countries are in favour of source protection, yet in practice the matter is different". She said that journalists are sometimes required to reveal the identity of their sources under emergency laws, or on the premise of fighting terrorism. (Ahmed 2015)

a. National Security/Anti-terrorism impacts

In the Syrian Arab Republic, a new media law was introduced in 2011 (Legislative Decree No 108, 2011 on media law) which circumscribes the media from publishing content that affects 'national security'. In Algeria, a new media law was introduced in 2012, which establishes limitations on coverage of state security (Algeria, 2012; CPJ 2012a).

b. Mass surveillance and targeted surveillance

While Internet engagement among the Arab states remains relatively low, the increasing numbers of users has corresponded with three countries introducing laws regulating use of the Internet since 2007, with potential implications for source protection.

In Egypt, litigation was pending (number 63055, judicial year 68) at time of writing against the Egyptian Ministry of Interior, challenging the Government's Internet monitoring activities. Such alleged surveillance is argued to contradict Egyptian laws regulating the investigation of evidence, which is limited to criminal activities or illicit acts (Provision 21 of Criminal Procedure Law).

In regards to Sudan, the 2009 Press and Printed Materials Act states (under the section Rights and Immunity of a Journalist that a journalist shall enjoy protection of sources (The Press and Press Printed Materials Act, 2009). At the same time, there is reported monitoring of online activities under the National Security Act of 2010 (Sudan, 2010; Freedom House 2014k; Reporters Sans Frontiers, 2014g; *Amnesty International* 2012).

13

c. Data retention/third party intermediaries

In Morocco, article 54 of the Draft Digital Law makes online service providers responsible for content created by users, which could indirectly impact on source confidentiality (Rhanem 2014).

d. Entitlement to Protection: Who is a journalist?/What is journalism?

Three of the countries studied demonstrated developments in relation to the question of who is entitled to claim source protection.

In October 2014, the Moroccan Government introduced a number of bills pertaining to the media. Among them was the "Status of Professional Journalists" bill that contains source protection provisions (RSF 2014c). Article 1 of the Status of Professional Journalists Bill stated that professional journalists are those "whose main occupation, regular and paid" is in "one or more publications, newspapers or periodicals published in Morocco, in one or more news agencies or in one or more broadcasting organizations, whose main office is located in Morocco" (Dahir n° 1-95-9 du 22 ramadan 1415 (22 Février 1995) portant promulgation de la loi n° 21-94 relative au statut des journalistes professionnels).

Sudan's 2009 Press and Printed Materials Act requires journalists to enrol in the Journalists Roll with the National Council for Press and Publications (NCPP) (see Freedom house 2014k; The Press and Press Printed Materials Act, 2009). Draft amendments to the act proposed in 2013 (Abbas 2013) would allow the authority to cancel journalists' licenses (Abubkr 2014).

In Algeria, under the new *Code de l'Information*, section 85 states that: "Professional secrecy is a right for the journalist and the director responsible, in accordance with laws and regulations" (*Code de l'Information de l'Algérie* 2012 Art. 85). The act defines a 'journalist' as someone whose income is solely derived from journalism.

e. Other digital dimensions

In Morocco in early 2015, recording equipment and other materials were confiscated from two French journalists (RSF 2015a). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

f. Anonymity issues

In Algeria, the 1990 *Code de l'Information de l'Algérie* recognised the right of Editors-in-Chief of publications to not disclose the real name of journalists or authors who write under pseudonyms, except when demanded by a competent authority following an official complaint (Article 39). Article 86 of the new 2012 media law requires that the journalist reveal his or her identity to their director and does not specify any exceptions (2012 *Code de l'Information de l'Algérie*).

The Mauritanian government ratified a Cybercrime Bill in 2014 (Jedou 2014), which has potential to impact on source confidentiality especially as regards the banning of encryption (see *Legal framework of the Mauritanian Information Society*, 2014).

g. Other dimensions

Four countries of the six reflecting developments demonstrated shifts in relation to source protection that are also relevant to non-digital dimensions. Morocco, Algeria and Sudan have been mentioned above. In Syria, a legislative decree states that the only institution permitted to ask a journalist to reveal her/his source is the judiciary in a secret session (Legislative Decree 108 for 2011). It is important to note the ongoing conflict and journalism safety issues in Syria, however, and concerns have been raised about the application of this decree (RSF 2011a).

Regional Conclusion

Over the period 2007-2015, 6 out of 7 countries examined in this UNESCO region experienced developments pertaining to source protection laws, across the relevant issues set out above. As with the African region, many of these developments have relevance to both digital and non-digital dimensions of source protection, but again there was not a lot of attention in the region to the purely digital space in the period under study.

6.3. Asia and The Pacific

In 2007, Banisar noted that: "A major recent concern in the region is the adoption of new anti-terrorism laws that allow for access to records and oblige assistance. There are also problems in many countries with searches of newsrooms and with broadly defined state secrets acts which criminalise journalists who publish leaked information". Developments since 2007 highlight increasing risks to source protection.

Of the 24 countries analysed in the Asia and Pacific region for this report, 18 (75%) have exhibited developments since 2007 that are potentially or directly relevant to the protection of journalists' sources.[14]

Countries with relevant developments 2007-2015:

- Australia
- Cambodia
- China
- India
- Indonesia
- Japan

14 Myanmar was not included in this study due to the methodology based on updating only the UNESCO Member States identified in the 2007 Privacy International report that was adopted as baseline research. However, there were noteworthy developments in the country between 2007-2015. These include 1) Surveillance (http://en.rsf.org/burma-surveillance-of-media-and-internet-17-05-2011,40296.html); 2) Journalists and others have faced organized cyber-attacks and attempts to infiltrate their e-mail accounts. (https://freedomhouse.org/report/freedom-world/2014/burma#.VPEr_MazJNI); 3) Amendments to Section 33 of the Electronic Transactions Law (2013) which criminalise "receiving or sending" information related to acts detrimental to state security, law and order, national solidarity, the national economy, or the national culture. Iran was also not included in this Study based on the methodology of updating the original baseline study countries, but the author also noted developments there that warrant further research.

- Kyrgyzstan
- Malaysia
- New Zealand
- Pakistan
- Philippines
- Singapore
- The Republic of Korea
- Sri Lanka
- Tajikistan
- Timor-Leste
- Turkmenistan
- Uzbekistan

There are a number of areas of concern in the Asia-Pacific region which have potential or actual bearing on source confidentiality.

a. National Security/Anti-terrorism impacts

In the Asia-Pacific region, there is an emerging trend where national security case law, legislation and/ or policy considerations demonstrate the potential to impact on journalists' source protection.

In China, journalists do not have the right to protect their sources under the Law of the People's Republic of China on Guarding State Secrets (Gov.cn 2010), nor under the Regulations on Secret-Keeping in Press and Publications (Xinhua 2013). China's National People's Congress considered an Anti-Terrorist Act at its meeting in March 2015. The Act contained a series of articles providing for legal large-scale monitoring and surveillance of citizens' communications, both online and offline. It also contained legal provisions that would enable the imposition of substantial restrictions on the activities, movement and ability of citizens to associate with any person suspected of terrorism (NPC 2015). At the time of writing, the draft law had been circulated for comment (Hewitt 2015).

In Macau, China, a Special Administrative Region of the People's Republic of China (PRC), national security laws were enacted in 2009 with offences punishable by sentences of up to 25 years (Macau, China: National Security Law, 2/2009). The law includes provisions covering state secrets (Article 5) without providing exceptions that could apply to journalists and whistleblowers (CECC 2009).

In Pakistan, investigative journalist Umar Cheema was kidnapped by unknown assailants in his country in 2010. His abductors took away his mobile phone and some of his sources later advised him about harassment they had experienced following his kidnapping, he told researchers on this study (Cheema 2014; Perlez J 2010; CPJ 2011).

In Australia, new anti-terrorism legislation (*National Security Legislation Amendment Bill* (No. 1) 2014) could see journalists jailed for up to 10 years for reporting on 'disallowed' national security stories, including those dependent upon confidential sources (Posetti 2015b; Williams 2014; See also Pearson & Fernandez 2015b). In 2015 the Federal Government classified information pertaining to asylum seekers on national security grounds. On the same basis, in mid-2015, the Australian Government criminalised the leaking of such information (Australian Border Force Bill 2015; Farrell 2015; Barns and Newhouse 2015).

In December 2013, Japan's parliament passed the *Act on the Protection of Specially Designated Secrets* (Act on the Protection of Specially Designated Secrets Act, No. 108, December 13, 2013). The law grants heads of state organs the power to designate as state secrets information connected to prevention of 'designated harmful activities', including matters in the realm of counter-terrorism, foreign affairs and defence. Unauthorized disclosure of such information is punishable by up to 10 years in prison (Freedom House 2014i). Whistleblowers and journalists found guilty of intentionally receiving such designated information can be jailed for up to five years under the Act (see Coliver 2014).

In Sri Lanka, the 1973 Press Council Act prohibiting disclosure of fiscal, defence, and security information, was revived in 2009. In June 2012, Sri Lankan police officers with support of a court order searched the offices of two news websites and confiscated equipment (*Colombo Telegraph* 2012; CPJ 2012c; Farook Thajudeen T. 2012; IFEX 2012; *New York Times* 2012). In 2012, the Sri Lanka Government amended the 1973 Sri Lankan Press Council Act so that websites would be governed by the same provisions that regulate the print media, which includes a prohibition on the publication of official secrets (Sri Lanka: Law No. 5 of 1973, Press Council Law [Sri Lanka], Chapter 378, 30 May 1973[15]).

In 2012, Malaysia passed the Security Offences (Special Measures) Act (SOSMA) 2012. In the act, the term 'security offence' is broadly defined as 'an act prejudicial to national security and public safety' (Spiegel 2012). SOSMA prohibits the possession or publication of 'detrimental' documents, which constitutes a security offence under the legislation. The term 'detrimental' is not defined. The legislation also permits police to intercept communications without judicial oversight. The Public Prosecutor is also granted authority to intercept postal articles and messages transmitted and received if it is likely to 'contain any information relating to the commission of a security offence'. (s6(1) of the Security Offences Special Measures Act; ARTICLE 19 2012).

b. Mass Surveillance and targeted surveillance

In China, communications between reporters, or with their sources via the Internet, or with digital devices, are subject to monitoring under Article 14 of the State Council Order No. 292 (2000), which grants government officials full access to information from providers of Internet services. In China (Hong Kong), the Interception of Communications and Surveillance Ordinance (ICSO Cap 589), enacted in 2006, requires a law enforcement agency in its application for authorization of interception or covert surveillance to state clearly whether journalistic material may be obtained in the operation (ICSO Cap 589 Schedule 3, Part 1 (ix), Part 2 (x), Part 3 (x)). In 2009, the Commissioner on Interception of Communications and Surveillance noted several incidents involving the interception of phone calls in which journalistic materials were obtained inadvertently. While the law itself does not require an agency to report such interceptions to the panel or the Commissioner,

15 Available at: http://www.refworld.org/docid/4be018692.html [accessed 28 February 2015])

the ICSO code of practice was amended in 2011 to require law enforcement agencies to notify the Commissioner of any operations that are likely to involve journalistic material or where such information had been obtained inadvertently. In 2013, after a two-year review of ICSO, the Hong Kong Government reported to the Legislative Council that it was drafting several legislative amendments, including one that would give the Commissioner access to materials produced under interception or surveillance, including journalistic material. However, at the time of writing, no new amendments had been introduced.

In the Philippines, the Supreme Court declared that s12 of the *Cybercrime Prevention Act* 2012 RA 10175 – which permitted the real time collection of data – was unconstitutional (Palatino, 2014; Danguilan-Vitug 2014).

Indonesia passed a state Intelligence Law in 2011. Article 32 of the legislation permits intelligence agencies to intercept communications without prior court approval, and without protections that could apply to journalistic communications (Freedom House 2013g, 2014f).

A law introduced in Pakistan in 2013, called the Investigation for Fair Trial Act 2013, gives the power to the state to intercept private communications in order to track suspected terrorists.

In New Zealand, the Search and Surveillance Act 2012 (New Zeland Parliamentary Council Office 2012) was introduced, legalising some forms of surveillance, extending surveillance powers to additional government agencies, and empowering judges to determine if journalists would be permitted to claim privilege (under Section 68 of the 2006 Evidence Act) in connection with warrants issued under the Act. While the Act recognises journalistic privilege, it states:

- "no privilege applies in respect of any communication or information if there is a prima facie case that the communication or information is made or received, or compiled or prepared,—
- (a) for a dishonest purpose; or
- (b) to enable or aid any person to commit or plan to commit what the person claiming the privilege knew, or ought reasonably to have known, to be an offence.

Also in New Zealand, the intelligence agency GCSB is reported to collect calls and Internet traffic in bulk and share this with the US National Security Agency (NSA), according to documents released by Edward Snowden and reported by *The Guardian* early 2015 (Manhire 2015).

In India, the Information Technology (Amendment) Act, 2008, allows the government to intercept, monitor, or decrypt computer information in the interest of "sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, or public order, or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence" (India, 2008; HRW 2013a; Bhatia, 2015).

Surveillance software linked to the state

As referenced earlier in this Study, in May 2013, researchers from Citizen Lab (Citizen Lab 2013) found evidence of FinFisher servers in 25 countries, including several in the Asia-Pacific region, which raised fears that government agencies may be using the software to

monitor (via backdoor access) their citizens. The deployment of such software directly can undermine legal protections designed to ensure confidentiality for journalists' sources.

c. Data retention and Third Party Intermediaries

In April 2015, a Pakistani parliamentary committee approved a bill that mandated service providers to retain data about Pakistanis' telephone and email communications for a minimum of one year. Called the Prevention of Electronic Crimes Act, it permits government authorities access to the data of Internet users without a requirement for judicial review, nor any exception for journalistic communications (HRW 2015b; PEC Bill 2015; HRW 2015b; RSF 2015b and RSF 2015c).

New data retention legislation in Australia demands that third party intermediaries store data for two years. The data retention Bill (Telecommunications and Interception Access Amendment Bill 2014), as it was proposed and initially approved by the Parliamentary Joint Committee on Intelligence and Security (APH 2015) did not provide safeguards that could provide for source protection. However, when the legislation was enacted in March 2015 it included an amendment (Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014) that requires agencies to seek a warrant to access journalists' communications with sources in certain cases. Transparency is however not required, nor is there a possibility to appeal the issuance of a 'Journalism Information Warrant'. Revelation of the existence (or non-existence) of such a warrant is punishable by a two-year jail term. Under the amendment, 'public interest advocates' will be appointed by the Prime Minister to advise on specific cases.

In Cambodia, in October 2014, the director of the Telecommunication Regulator of Cambodia (TRC), ordered 12 mobile phone and Internet providers to be studied by police. Information analysed included billing records, network information, and data logs (Pheap A and Wilwohl J 2014; Telecommunication Regulator of Cambodia 2014).

d. Entitlement to protection: Who is a journalist/What is journalism?

Five of the 24 countries studied in the Asia-Pacific region reflected developments in policy and case law pertaining to definitions of 'journalist' and 'journalism'.

In Australia, six out of nine jurisdictions (at federal level and in New South Wales, Victoria, Western Australia, the Australian Capital Territory and Tasmania) have introduced shield laws. Three out of those six are potentially broad enough to cover bloggers (*Evidence Act 1995* Cth, s126G (1), *Evidence Act 2001* ACT, s 126J, and *Evidence (Journalists) Amendment Bill 2014*, Part 8A—Journalists 72—Interpretation) (Fernandez 2014). Also in Australia, the protections for journalistic data contained within the Telecommunications and Interception Access Amendment Act 2015 are afforded to "a person who is working in a professional capacity as a journalist". Similarly, sources who might benefit from this amendment are only covered if their interactions are with "professional journalists" in the course of professional news media production (Hurst 2015).

The Banisar (2007) report documented the codification of 'journalist' in a New Zealand shield law in 2006 (Evidence Act 2006, s 68). Significantly, in 2014, a High Court judge extended the protection to a political blogger who was deemed to be a journalist, and his blog was accepted as a news medium. But it is important to note that the court ordered the source

to be revealed as the 'public interest' involved in this particular case favoured disclosure (*Slater v Blomfield* [2014]). The decision also relied on tests like 'regularity' and 'effort' of news production which could exclude occasional acts of journalism. Nevertheless, it does offer a broader definition of journalistic acts.

In 2010, the Chinese Government introduced a national "Qualification Examination" for Journalists. Administered by the General Administration of Press and Publication, the government's main regulator of the press, all practicing and prospective journalists must pass a new qualification exam. In addition to screening of journalists, this development excludes bloggers and other digital communicators from claiming ethical obligations under the China News Workers Code of Professional Ethics.

In 2007, a court required a Reuters journalist to reveal her source in Singapore (*Tullett Prebon (Singapore) Ltd and Others v Spring Mark Geoffrey and Another* [2007] 3 SLR 187; [2007] SGHC 71). However, in 2014, the Singaporean Court of Appeal protected a blogger from revealing his source, although a lower court had decided that he was not a journalist (*James Dorsey Michael v World Sport Group* [2014] SGCA 4).

In Timor-Leste, the 2014 Press Law defines the term 'journalistic activity' to encompass research, collection/selection of information; processing and dissemination of information in the form of written text, sound or image to the public through disclosure in the media. (*Decree No. 10/III Media Act*, Article 2, a)). However, the term 'journalist' is limited to a professional who is primarily engaged in journalism. The profession of journalist under this media law is further constrained by the requirement of a professional license (Ibid, article 13, i)) which is issued and controlled by a press council, internship requirements and a Bachelors-level qualification in the field. Shortly after being approved by Timor Leste Parliament, the Press Law was referred to its highest court by President Taur Matan Ruak, which deemed some sections unconstitutional in August 2014 (East Timor Law and Justice Bulletin 2014; Pacific Media Centre 2014).

e. Other digital developments

In June 2014, the State Administration of Press Publication Radio Film and Television (SAPPRFT) – the agency responsible for oversight of China's media - issued new measures aimed at preventing Chinese journalists from sharing certain information on their personal blogs and social media accounts, and with foreign news media. The new provisions forbid journalists and media employees from sharing certain state secrets, trade secrets, intellectual property and undisclosed information obtained during professional activities (Politics 2013). All journalists are required to sign an agreement to pledge compliance with the regulations.

In October 2014, police seized digital devices from the home of New Zealand investigative journalist Nicky Hagar (Fisher 2014). At the time of writing (July 2015), Hagar was challenging the legality of the raid in the High Court of New Zealand, citing concerns about source protection.

There were two searches of Australian newsrooms during the period by the Australian Federal Police (AFP). In both cases, the searches involved targeting journalists' computers and mobile phones to access data (*The World Today* 2011; Bartlett 2015). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

In the second incident, in 2014, police apologised to a TV station in Sydney after searching the newsroom in an attempt to establish if a convicted drug trafficker had been paid for an interview in a 'proceeds of crime' investigation. Documents and computers were seized during the search, but the Federal Court overturned the warrants that were issued to procure them, and the items were later returned (ABC NEWS 2014). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

In Kyrgyzstan in 2008, authorities with support of a court order searched the offices of a newspaper, confiscating financial records and computers in a criminal investigation (CPJ 2008; RSF 2008; WAN-IFRA 2008). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

In Uzbekistan, a freelance journalist was detained briefly at Tashkent airport in August 2011 and had digital equipment taken (RSF 2011b; Freedom House 2012h; Ferghana 2011). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

f. Anonymity issues

China has enacted new regulations requiring real-name registration for use of digital and social media. In December 2012, the National People's Congress (NPC) approved a law requiring real-name registration for Internet access. The real-name registration system was subsequently enacted for the social network Sina Weibo in 2012 (Xinhua 2012), and for instant messaging systems in 2014. In April 2013, The Ministry of Industry and Information Technology (MIIT) drafted a law requiring real-name registration for setting up any phone line or mobile connection in the country. Four months later, China's three major telecommunication companies began to require all subscribers to register with their real name and national ID number. In January 2014, the State Administration of Radio, Film, and Television (SARFT) issued a notice to video-hosting websites stating that anyone who uploads a video to the Internet must be registered using their real name. In 2015, the State Internet Information Office announced the implementation of a comprehensive real-name registration and oversight system, which covers microblogs, Baidu's Tieba (discussion) forums, and other sites with user-generated content (CAC 2015).

In the Republic of Korea in 2012, the Constitutional Court rejected a 'real name law' introduced in 2007 on the grounds that it reduced freedom of speech (Ramstad 2012).

g. Other dimensions

The China News Workers' Code of Professional Ethics (Xinhua 2009) stipulates that the reporters should defend the legal rights of sources. It is a voluntary code. Chinese courts can require journalists to reveal the identity of sources in a criminal case. According to Beijing-based lawyer Shi Hongying, all citizens have the obligation to testify in criminal cases according to Article 60 of the criminal law (Fawan 2013).

A company filed a suit in 2012 against the Guangzhou-based *Southern Weekend* newspaper and *The Beijing News*, charging that the papers printed articles that defamed the organization. The court ruled against the papers on the grounds that their articles contained anonymous sources and that the papers had refused to disclose the sources to the court (China File 2014).

In Hong Kong, China, the Interpretation and General Clauses Ordinance was used in 2013 by the Independent Commission Against Corruption which went to court to apply for orders to try to compel two media organizations to produce interview tapes and notes for its officers to use in criminal investigations. It was the first time that a law enforcement agency had resorted to production orders since the enactment of the 1995 law, which offers additional protection to journalistic material. The applications were ultimately rejected by a judge (Buddle 2015).

A number of cases have tested the protections of the shield laws passed in six Australian legal jurisdictions since 2011. A recent judgment deemed that discovery orders were permitted to uncover sources if the only 'tangible risk of adverse consequences' was the risk of a source being sued for defamation (Liu v The Age Company [2012] NSWSC 12) (Fernandez 2014). In 2014, an Australian academic launched legal proceedings against a publication in an attempt to force the revelation of the source of published emails containing remarks he made. The court rejected claims of a breach of privacy levelled by the litigant, and the application to reveal the source was dropped (New Matilda 2014). In another case (*Newspaper Ltd v Bond, 2009; Hancock Prospecting v Hancock 2009*), the Supreme Court of Western Australia dismissed a private individual's request for a journalist to hand over source information (Lidberg 2013). A separate bid by the same individual to pursue sources cited in an unauthorised autobiography failed on the basis of the precedent set in the first case and in terms of the applicability of Western Australia's new shield laws (Weber 2014; *Hancock Prospecting v Hancock*, 2013; WASC 290).

Also in Australia, it was reported by *Guardian Australia* in 2015 that several Government agencies had referred cases of confidential source-dependent journalism, about issues affecting asylum seekers, to the Australian Federal Police (AFP) for investigation into "unauthorised disclosure of commonwealth information", with a view to identifying the sources and other whistleblowers (Farrell 2015 a).

In Tajikistan, a new media law was introduced in 2013 that effectively reversed an obligation on journalists to identify sources (See Article 32 'Journalists' Duties', The Law of the Republic of Tajikistan). In Article 26, the new law imposes a legal obligation upon journalists not to reveal their sources (See related discussion in Case Study 2; ARTICLE 19, 2014)

In Timor-Leste, the National Congress of Journalism, an historic gathering of the country's journalists approved a new journalism Code of Ethics in 2013 (Republica Democratica De Timor-Leste, 2013; Pearson 2013). This was enshrined via a new media law that was approved in the National Parliament in May, 2014. Article 19, subsection 4 of the Code of Ethics protects the journalists' right to professional secrecy, stating that journalists 'may not be forced to disclose their sources of information, except when so ordered by a court under the criminal procedure law' (Decree No. 10/III).

In another development, Turkmenistan introduced a media law in 2013. Among other things, the duties of a journalist are defined, and these include the need to maintain the confidentiality of information and/or its source (article 31, subsection 5). Journalists are not entitled to identify the person who provided the information on condition of non-disclosure of her/his name, except in the case of a corresponding demand from the court (article 39). The law had not been tested at the time of writing.

In Malaysia, a Court of Appeal judgement found that a reporter did not have to reveal the sources of a story in a defamation case (Mageswari, 2014). In a second case, in 2010 The Star Publications sought judicial review on a case in which a journalist refused to hand over

notes for examination (Hong Chieh 2010; Loh 2010). The review was granted but The Star later withdrew the challenge (Sun Daily 2010).

Regional conclusion

The region experienced developments over the period in 18 of 24 countries surveyed, as regards the issues of a) national security/anti-terrorism impacts; b) Surveillance; c) Data retention/handover and the role of third party intermediaries; d) Questions about entitlement to claim source protection; e) Other digital dimensions (digitally stored journalistic communications being seized), f) Anonymity issues, and g) Other dimensions.

6.4. Europe and North America

i. Europe

"The protections are strongest in Europe where the European Court of Human Rights has specifically found in favour of the right of protection and the Council of Europe has issued detailed guidelines on the protections" (Banisar 2007 p. 13).

Since 2007, developments have been identified in 23 European countries, out of the 36 (64%) examined as a subset of UNESCO Member States identified for study.

The 23 countries[16] exhibiting developments in regard to source protection between 2007-2015 are:

- Armenia
- Austria
- Belarus
- Bulgaria
- Czech Republic
- Estonia
- France
- Georgia
- Germany
- Hungary

16 Slovenia is also a UNESCO State where further research is recommended. It fell outside this Study's scope, however the author noted relevant developments, as reported by a Slovenian academic survey respondent, including limits of the existing legal source protection framework in the digital era. Additionally, an investigative journalist faced criminal charges after publishing information allegedly based on leaks (OSCE 2014 http://www.osce.org/fom/151736). She was called to reveal her sources during the trial but the prosecutor withdrew the charges before a verdict was delivered http://globaljournalist.org/2015/04/slovenia-drops-state-secrets-charge-against-reporter/ Similarly, a 2010 case in Serbia is noteworthy – it was also not included in this study on methodological grounds (C.f. the case of Bojovic and Spasic). http://journalism.cmpf.eui.eu/discussions/europes-journalists-caught-in-widening-national-security-net/).

- Iceland
- Ireland
- Israel
- Lithuania
- Netherlands
- Poland
- Portugal
- Russian Federation
- Slovakia
- Switzerland
- The former Yugoslav Republic of Macedonia
- Turkey
- United Kingdom of Great Britain and Northern Ireland

The Media Legal Defence Initiative's Peter Noorlander, interviewed for this study, commented that there was a steady stream of cases before the European Court of Human Rights, where police had used search and seizure laws and argued that not all journalistic material qualified as confidential. He added: "The European Court has held a high line and declared violations of source protection and the right to freedom of expression in (nearly) all these cases, but the States concerned have been slow to implement them" (Noorlander 2015).

The Organisation for Security and Cooperation in Europe's (OSCE) *Safety of Journalism Guidebook* (Horsley 2012) noted "persistent threats of prosecution which contradict the accepted right to the protection of sources are of concern". The OSCE's Representative on Freedom of the Media, Dunja Mijatović, has also routinely condemned threats to legal source protection frameworks in Europe and North America during the period.

a. National Security/Anti-terrorism impacts

In January 2015, the attack on the *Charlie Hebdo* newspaper in Paris, European Interior Ministers issued a joint statement in the immediate aftermath of the attack explaining the need to take measures in the interests of national security (EU 2015; Posetti 2015a).

Earlier, the Snowden revelations also led to actions by governments in Europe that have impacted on the protection of sources, in instances such as the requirement that *The Guardian* destroy hard drives (Majumdar 2013), and the detention of a journalist's partner at Heathrow airport, along with the concurrent seizure of journalistic material (Bowcott 2014).

In early 2015 *The Guardian* published a new cache of Snowden files that reported that a UK Government Communications Headquarters (GCHQ) information security assessment listed "investigative journalists" in a threat hierarchy (Ball 2015). In June 2015, the UK's Independent Reviewer of Terrorism Legislation, David Anderson QC published the report

A Question of Trust: Report of the Investigatory Powers Review (Anderson 2015) which stated that: "… the ability of a whistleblower to reveal state misconduct and of a journalist to report it requires an assurance that the journalist's sources will not be made known to the state" (See also discussion of Anderson's recommendations in the Mass Surveillance and Data Retention sections below).

Also in the UK, the Terrorism Act (2000) has been used to require materials from journalists who investigated or interviewed terror suspects. In 2008, a freelance journalist was required to hand over data pertaining to communications with a terror subject during research for a book. The High Court conducted a judicial review of the case and required the journalist to hand the material directly gathered from the suspect, but further ruled that he was not required to give up materials gathered from other sources (Shiv Malik v Attorney General [2008] EWHC 1362) (Fitzsimmons 2008).

In 2009, Germany adopted an anti-terrorism law that provided greater power to authorities (namely the BKA – Germany's Federal Criminal Police Office) to conduct covert surveillance (Spiegel Online International 2008). Paragraph 20 of the law provided journalists' communications, along with those of doctors and lawyers, to be intercepted in the absence of a requirement for probable cause if a public interest was detected (Hawley 2009, see also McGauran 2009).

The French Senate passed new anti-terrorism legislation in June 2015 (Loi renseignement 2015) that expanded surveillance powers and granted law enforcement agencies special surveillance powers, including new monitoring processes and methods of investigation with limited judicial oversight (OSCE 2015).

Hungary introduced new media legislation in 2010 in terms of which a journalist protecting a source (or associated data) could be fined up to €661,000, and a publisher fined €180,000 if there was an issue of 'state security' (Mayr 2011). This legislation was then amended in 2012 following a Constitutional Court judgement. According to the amendment, sources must be disclosed only if they provide evidence that would be necessary to resolve a criminal case. Judges enjoy a large margin of discretion in balancing the journalist's obligation to protect the source and the need to disclose the information in order to solve a criminal case (European University Institute: 2014; Falchetta 2015).

b. Mass surveillance and targeted surveillance

In France, in 2013, article 13 of a new law was introduced, enabling significantly expanded government surveillance of French citizens (Assemblée Nationale (b): 2013). The new law allowed a wide range of public officials (including police, gendarmes, intelligence and anti-terrorist agencies, as well as several government ministries) to directly monitor computer, tablet and smartphone use in real time, and without prior authorisation, for the purpose of gathering metadata (Willsher 2013). This legislation contains no exemptions that could apply to journalistic communications.

In July 2015, CNN reported that NSA surveillance of German journalists and their sources had led to a foreign agency revealing the identity of one of these sources to the German Government in 2011 (Tapper 2015; *Der Spiegel* 2015).

In February 2015, an opposition leader in the Former Yugoslav Republic of Macedonia claimed that he had obtained evidence that over 20,000 citizens had been subjected to

unauthorized surveillance (IFEX 2015). Among the reported targets were more than 100 journalists. According to Deutsche Welle, the journalists were invited to the opposition party's headquarters to collect folders and documents filled with transcripts of their conversations spanning a two-year period (Georgievski 2015).

An instance of wiretapping of journalists in Lithuania was declared illegal by the Vilnius Regional Court in August 2014 (OSCE 2014c). The Vilnius District Court had sanctioned wiretapping of BNS news agency journalists at the end of 2013 at the request of the Special Investigation Service following an article (based on confidential sources), which was published by BNS. The regional Court also found that secret surveillance, searches and an order to reveal the sources of information were unlawful.

In 2014, the UK's Bureau of Investigative Journalism (BIJ) and a journalist filed an application with the European Court of Human Rights (Bureau of Investigative Journalism and Alice Ross v. The United Kingdom (2014) 62322/14) to rule on whether UK legislation properly protects journalists' sources and communications from government scrutiny and mass surveillance. The case argued that bulk collection of communications data, using methods such as Internet cable tapping, breaches international human rights law (Oldroyd 2014). It was argued by the Bureau that the UK Government's practices of intercepting, collecting, storing and analysing data, including metadata, under the Regulation of Investigative Powers Act 2000 (see discussion on RIPA in the Data Retention section below) make it substantially harder for journalists to guarantee confidentiality to their sources (ECHR 2014).

A number of other surveillance developments with relevance to source protection have occurred in the UK. The country's Investigatory Powers Tribunal (IPT) found in early 2015 that the regime governing the sharing of electronic communications collected by Britain and the US had been unlawful until disclosures were made by the UK's Government Communications Headquarters agency (GCHQ) in 2014 (06/02/15 IPT/13/77/H Liberty & Others vs. the Security Service, SIS, GCHQ; Bowcott a 2015). However, the NSA-GCHQ relationship was deemed legal from the point at which it had been disclosed (05/12/14 IPT/13/77/H Liberty & Others vs. the Security Service, SIS, GCHQ.) The litigants announced their intention to appeal to the European Court of Human Rights.

Also in 2015, the UK's Home Office published a Draft Equipment Interference Code of Practice (UK Government 2015) which references journalistic source confidentiality and suggests that particular consideration should be given when accessing such data through means it describes as "equipment interference". Point 3.23 states that: "Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking". The Code requires agencies to carefully consider the necessity and proportionality of moves to access such data, to detail the reasons for doing so, to destroy the data when it is no longer needed, and to take reasonable steps to ensure the data is marked 'confidential' if it is handed to outside bodies. However, it does not indicate a data retention time limit (Travis 2015).

Further in 2015, the UK parliament's Intelligence and Security Committee (ISC) released a report titled *Privacy and Security: A modern and transparent legal framework*, which noted that the authorities had capacity to trawl massive sets of personal data without statutory oversight. It also found that the UK's legal framework has developed in a "piecemeal" manner, was "unnecessarily complicated" and lacked transparency (ISCP 2015).

In his report released in June 2015, the UK Independent Reviewer of Terrorism Legislation, David Anderson QC, recommended judicial review of requests for interception warrants to acquire communications data of people who handle privileged or confidential information, including journalists. Anderson also proposed that the authorisation should be flagged for the attention of the Independent Surveillance and Intelligence Commission (ISIC) in the interests of accountability and transparency. Recommendation 68 of his Report states: "If communications data is sought for the purposes of determining matters that are privileged or confidential such as…the identity of or a journalist's confidential source, the Designated Person should be obliged either to refuse the request or to refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request" (Anderson 2015). At the time of writing, the UK Government had not committed itself to Anderson's recommendations (Sparrow 2015). However, in 2015 it indicated that it would soon bring forward new legislation (Lomas, 2015).

When the research for this Study was completed in July 2015, there were several other significant UK cases pertaining to surveillance pending in UK and European courts with potential implications for source protection in the digital age.

In Bulgaria, in the course of an ensuing government investigation into the beating of an investigative journalist, mass wiretapping of journalists and government officials was revealed (Basille 2009; OSCE 2008; Slate 2009).[17]

According to the Russian state news agency Ria Novosti (РИА Новости), the number of intercepted telephone conversations significantly increased between 2007 and 2012. While the Federal Security Service (FSB) is the principle agency responsible for communications surveillance, several other Russian security agencies can access a surveillance system in accordance with provisions on privacy in the Constitution (article 23), the federal law on surveillance (Об оперативно-розыскной деятельности) and other laws (Constitution of the Russian Federation 1993; Federal law on surveillance N 144-ФЗ; Federal Law on communications N 126-ФЗ; Ria Novosti 2013; Lewis J A 2014; World Policy 2013).

Polish newspaper Gazeta Wyborcza published an article in 2010 claiming that a number of political journalists were under illegal surveillance. Between 2005 and 2007, Polish intelligence agencies obtained and analysed the telecommunications data from the author of the article (Szymielewic & Walkowiak 2014). In 2011, the journalist took civil action against one of the agencies, and in 2012, a Warsaw district court ruled that the use of his telephone data violated his right to privacy and constituted a breach of his freedom of expression rights. The court ordered the agency to apologise to the journalist and required it to delete all data relating to him.

In Turkey, a law expanding the powers of the National Intelligence Agency came into force in April 2014 which permits collection of Internet traffic data (Turkey 2014).

Belgium's Law on Protection of Journalists' Sources (2005) prohibits the use of 'any detection measure or investigative measure' of any protected media person unless it is authorized by a judge under the same restrictions as required to compel a journalist to reveal his/her source of information.

17 There have been legislative developments subsequently:
http://sofiaecho.com/2009/12/22/834248_electronic-communication-act-amendments-for-first-reading-in-parliament ;
http://history.edri.org/edrigram/number8.1/bulgarian-protests-data-retention ;
http://www.novinite.com/articles/167509/Bulgarian+Parliament+Adopts+Changes+to+Electronic+Communications+Act;
http://www.bta.bg/en/c/ES/id/1044976

c. Data retention/Third party intermediaries

Protection of journalistic sources in relation to data retention and access, and in relation to Internet companies, was the subject of debate in the UK in 2014/2015, following two high profile cases where police accessed journalists' communications records with the explicit aim of identifying sources, using the Regulatory Investigative Powers Act (RIPA) to do so (Turvill 2014).

Confidentiality of journalistic sources in the UK is protected by the Police and Criminal Evidence Act (PACE) of 1984 which excludes certain material from seizure, including:

- Journalistic material which a person holds in confidence and which consists—

i. of documents; or

ii. of records other than documents.

Journalistic material is defined as follows:

- A person holds journalistic material in confidence for the purposes of this section if—

a. He [or she] holds it subject to such an undertaking, restriction or obligation; and

b. It has been continuously held (by one or more persons) subject to such an undertaking, restriction or obligation, since it was first acquired or created for the purposes of journalism.

The Regulation of Investigative Powers Act (RIPA 2000), originally intended to safeguard national security as an anti-terrorism measure, allows police to circumvent the PACE. *The Sun* newspaper has applied to the Investigative Powers Tribunal for a review of the Metropolitan Police's use of RIPA to access and analyse mobile phone records (O'Carroll 2014). It is alleged that the police action breached Article 10 of the European Convention on Human Rights in ordering Vodafone to hand over the records (Ponsford 2015c). Since the application was lodged, it has been revealed that the phone records of two other *Sun* journalists were also intercepted in the course of the same police investigation (Ponsford & Turvill 2015).

Also in 2012, Essex police accessed the phone data of two Mail on Sunday journalists in the course of a leak investigation into the newspaper's coverage of speeding fines issued to a former cabinet minister (Greenslade 2014).

A report assessing the nature of the RIPA surveillance powers was published in mid-2015 by the Interception of Communications Commissioner, Sir Anthony May (May 2015). It found that the RIPA legislation 'did not provide adequate safeguards to protect journalistic sources' (Press Gazette 2015). Specifically, it found:

- In the three-year period covered by the inquiry, 19 police forces sought communications data in relation to 34 investigations into suspected illicit relationships between public officials (sources) and journalists.

- 608 applications were authorised to seek this communications data

The result was that police forces were able to secretly view phone records of 82 journalists during the period, allowing them to identify the journalists' sources (Ponsford 2015a). May's report recommended that: "Judicial authorisation is obtained in cases where

communications data is sought to determine the source of journalistic information" (May 2015; *The Guardian* 2015). The report also stated that that the police forces did not give the question of necessity, proportionality and collateral intrusion sufficient consideration (Bureau of Investigative Journalism 2015).

In May 2015, in response to growing concerns about the impact of RIPA disclosures on journalistic source protection, temporary measures were introduced to amend the UK Serious Crime Bill. The new rules required the police force to seek judicial approval before viewing a journalist's phone records in a criminal investigation.[18]

In July 2014, the Data Retention and Investigative Powers Act (DRIPA) was fast-tracked into law, requiring bulk retention of data for 12 months, and extending the definition of telecommunications services in RIPA to include email and other Internet-based services, without exceptions for material covered by legal, medical or journalistic professional confidentiality. In July 2015, the High Court of Justice declared bulk data retention under the DRIP Act illegal (Case No: CO/3665/2014, CO/3667/2014, CO/3794/). According to the judgement, aspects of the Act were unlawful because they breached Articles 7 and 8 of the EU Charter of Fundamental Rights (BBC 2015a). They declared that section 1 of the act "does not lay down clear and precise rules providing for access to and use of communications data" and should be "disapplied". The court identified two key problems with the law: 1) it did not provide for independent court or judicial scrutiny to ensure that only data deemed "strictly necessary" is examined 2) there was no definition of what constitutes "serious offences" in relation to which material can be investigated. They suspended their order until March 31 2016 in order to "give parliament the opportunity to put matters right". The Home Office security minister announced that the UK Government would seek to appeal the judgement (Bowcott 2015b).

In April 2012, Austria introduced a data retention law, which required telecommunications companies and Internet service providers to store user data for up to six months. This was then ruled unconstitutional by the Austrian Constitutional Court, as it violated fundamental European privacy rights (PC World 2014). A 2012 Security Policy Act enabled monitoring, wiretapping, filming and geolocation of individuals by state authorities (Freedom House 2014a).

In Germany, a data retention law passed in 2008 was overturned in 2010 by the Federal Constitutional Court and declared unconstitutional because it breached German privacy laws. The law had required telecommunication companies and Internet-service providers to store citizens' communications data, including their Internet browsing history, for up to six months. Additionally, it permitted the wiretapping of lawyers, doctors, and journalists under certain circumstances. The Supreme Court found that there were insufficient safeguards and oversights and it ordered that all previously retained data be deleted immediately (Freedom House 2011a; Der Spiegel 2010; ERDI 2010).[19]

In 2011, however, Germany's Constitutional Court found that the legislature did not have to provide journalists the same confidentiality protections applied to other professions, such as lawyers. (Freedom House 2012a).

18 See also the discussion of the News of the World 'phone hacking' scandal in the next section of this report

19 Romania is not covered in this Study's analysis on methodological grounds, but it can be noted that the country's Constitutional Court also twice ruled that country's data retention laws unconstitutional (in 2009 and 2014) c.f. https://edri.org/romania-aftermath-of-second-ccr-data-retention-ruling/

At the time of writing, the Polish Constitutional Court was considering six complaints from the Ombudsman and Prosecutor General arguing for limitations on the powers available to intelligence and law enforcement operatives in Poland. In 2012, the mandatory data retention period of two years was reduced to 12 months. Two bills - one seeking to limit intelligence agencies' access to Polish citizens' telecommunications data, and the other providing for oversight of intelligence agencies' complaints processes – were under consideration in 2014 (GISWatch 2014). (See also the case of mentioned under the surveillance section above).

Dutch lawyers, journalists, privacy organizations and publishers were, at the time of writing, taking legal action against the Dutch government in opposition to legislation that requires telecom firms to store phone and email information (NU.nl 2014; DutchNews.nl 2014). Legal counsel for the complainants alleged that the legislation conflicts with judgments of the European Court of Justice in 2014.

The European Court of Justice earlier found the Irish Data Retention Directive was invalid on the grounds that it "interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data" (NU.nl 2014). In response to criticism from these groups in late 2014, the Dutch Government amended the provisions, but still kept the data retention legislation on the grounds that it was needed for investigation and prosecution of serious criminal offenses (Rijksoverheid 2015).

On 23 April 2014, the Slovak Constitutional Court preliminarily suspended Slovakian implementation of the 2006 European Union Data Retention Directive, which had been given force in Slovakia under the Act on Electronic Communications. The suspension followed a case brought in September 2010 by the European Information Society Institute (ElSi) against data retention in Slovakia (Husovec & Lukic 2014). The laws are still formally valid, but have no legal effect until the Court decides on the merits of the complaint.

In Belarus, several by-laws and governmental decrees have been approved in recent years, including one that requires Internet service providers to identify all Internet connections and to store data about their customers, and the websites they visit (Aliaksandrau & Bastunets 2014). Telecommunications companies must record the passport details of people who buy SIM cards Internet café staff are required to photograph users, and operators of all cafes and hotels are required to register users before supplying them with Wi-Fi access.

Georgian journalists enjoy constitutional and federal level legal protections regarding confidentiality. However, a clause limiting public agencies' direct access to surveillance data was removed from a cybersecurity law in August 2014 (IDFI 2014). The first report of the Personal Data Protection Inspector (a government authority established in 2013) on the State of Personal Data Protection noted problems of processing of a large amount of data without proper legal grounds; the illegal disclosure of personal information; and failure to meet legal requirements related to video surveillance (Freedom House 2014m).

d. Entitlement to protection: Who's a journalist? What is journalism?

A new law adopted by the Former Yugoslav Republic of Macedonia at the end of 2013 addressed the question of the definition of 'journalist' and, therefore, to whom source protection applies. The definition of journalist emphasises official contractual ties to a legacy-media newsroom (IREX 2014: 73).

Citizenship has been relevant to the issue of who is eligible to have protection of confidential sources. Wikileaks' Editor-in-Chief, Julian Assange travelled to Sweden in 2010, before moving his organisation's servers to the country. Wikileaks wanted to benefit from the country's stringent whistleblower and source protection laws. In Sweden, if a website registers with the public authorities and can prove it has an Editor-in-Chief, then it can be certified to become legally obliged to protect confidential sources (Euractiv: 2010). Under Swedish law, Assange would have needed to become a Swedish citizen in order to apply for source protection coverage. (See also detailed discussion of the status of source protection in Sweden in the digital age in Thematic Study 2).

e. Other digital dimensions

In Georgia in 2011, five photojournalists were arrested and had computers, mobile phones and other reporting equipment reportedly seized (Robinson M 2011; RSF 2011c). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

In June 2014, a Polish magazine was repeatedly searched by the Prosecutor's Office and Internal Security Agency officers (OSCE 2014c). The Editor-in-Chief was required to hand over recordings and electronic devices to the authorities during the searches. This example is not provided with the presumption that confidential journalistic data was unduly exposed.

In July 2013, GCHQ officials in the United Kingdom oversaw editors destroying laptops containing the Snowden files (Fitzsimons et al 2014). *The Guardian* stated that it had been threatened with legal action by the Government to recover the laptops unless they agreed to destroy the data (Borger 2013; Harding 2013). By agreeing to destroy the laptops, *The Guardian* believed it was protecting both its source and its reporters.

In Hungary, the Act CLXV on Complaints and Whistleblowing came into force in January 2014. The new law ushered in an electronic whistleblowing system operated by the Commissioner for Fundamental Rights (the ombudsman). Whistleblowing reports are registered by an anonymised code and published on the Internet in a form designed to be accessible to all, without any data relating to the identity of the actual whistleblower. The process then involves the ombudsman transferring the report to the competent authority for investigation (Barker Exchange 2014). The Act emphasizes the protection of the whistleblower as required by the UN Convention against Corruption in Articles 32 and 33 (UN 2003). The whistleblowing facility follows a 2007 Pricewaterhouse Coopers study that found that whistleblowing had been very beneficial to Hungary in fraud detection and reporting economic crime. This model parallels similar systems established by news publishers in US, Africa, Latin American and Europe (see Thematic Study 1).

Publishers and source protection

The UK 'phone hacking' scandal (Davies 2014), revealed by *The Guardian*, that began at *News International's News of the World* and included a number of other UK tabloid publications, raises several complex issues in regard to confidentiality, privacy and protection of sources. The original scandal revealed that journalists using private investigators had illegally intercepted the mobile phone messages of celebrities and other citizens. This led to a number of high profile inquiries into the ethics of the UK tabloid press and several police investigations that ultimately ended with the jailing of multiple journalists and their police sources (BBC 2014).

The investigations also revealed that tabloid publications had illegally paid public officials and police as sources of confidential information. Under growing pressure, News International executives established their own investigation which worked with Pricewaterhouse Coopers to assemble a database of 300 million emails and other documents relating to journalists' phone records and expenses (Ellison 2012). Many of these records were then turned over to police by News International. These records have since been used by police to identify sources, and convict both journalists and their sources (BBC 2015b). There is also some evidence that police have used the data given to them by News International to investigate police who gave information to journalists but who were not paid (Laville 2013) – that is, confidential sources who were not in a corrupt relationship with the press. News International executives have justified the voluntary turning over of records to police (Ellison 2012), but have been criticized by both internal (O'Carroll 2012) and external critics (Crook 2014).

Also flowing from the 'phone hacking' scandal was the Leveson Inquiry into the practices of the British press. In 2012, the Leveson Report (Leveson 2012) recommended weakening the source protection rights of journalists by suggesting that the definition of excluded material in the Police and Criminal Evidence Act 1984 (PACE) be narrowed. PACE stipulates the conditions under which police can seek to obtain unpublished confidential source material (Phillips 2014). The Report recommended that protection should only be afforded to journalistic material "if it is held, or has continuously been held since it was first acquired or created, subject to an enforceable or lawful undertaking, restriction or obligation." This implies the need for an explicit obligation of confidence between a journalist and a source in order for protection to be upheld.

f. Anonymity issues

No specific developments were registered by the researchers over the period under focus.

g. Other dimensions

According to Banisar (2007), 40 countries - the vast majority of countries in Europe – had adopted some form of legal protection for journalistic sources by 2007, the only exceptions being Ireland, the Netherlands, Slovakia and Greece, and smaller jurisdictions such as the Holy See and Andorra. The following paragraphs update this 2007 assessment.

In the Republic of Ireland, protection of journalistic sources is not dealt with via statutory law. Pronouncements by the European Court of Human Rights remain the common reference point for Irish courts. For example, in 2007, two journalists from the Irish Times who were ordered by Tribunal of Inquiry to produce the original of a leaked letter published in the paper, were told by the Irish High Court to comply (Mahon Tribunal v Keena & anor [2009] IESC 78). An appeal by the journalists to the Irish Supreme Court unanimously reversed the order of the High Court in 2009. The Supreme Court held that the High Court had not 'struck the balance between the journalistic privilege derived from the exercise of the right to freedom of expression of the appellants and the public interest of the Tribunal in tracing the source of the leak'. However, the Supreme Court continued:

> *"The unilateral decision of a journalist to destroy evidence with intent to deprive the courts of jurisdiction is, as the High Court has held, designed to subvert the rule of law. The Courts*

> *cannot shirk their duty to penalise journalists who refuse to answer questions legitimately and lawfully put to them"*

The Supreme Court held that due to 'exceptional circumstances' - that is, the destruction by the newspaper of the documents - the *Irish Times* had to pay all costs (Cormaic, 2014) which totalled €600 000 (Greenslade 2009). The *Irish Times* appealed the costs decision to the European Court of Human Rights which rejected the application.[20]

Slovakia legally recognised protection of journalists' sources with the Press and News Agency Act No. 167/2008, and the subsequent amendment act no. 221/2011 (National Council of the Slovak Republic 2011). Section 4 of the Act on Protection of Information Sources and Content states:

> *The publishers of periodicals and press agencies must not disclose the source of information acquired for publication in a periodical, or an agency news service, or any part of the content of such information which would enable the identification of the source if requested not to do so by the natural person who provided the information, and must ensure that the disclosure of the content of the information does not breach the rights of third parties; they are obliged to take the necessary precautions in the handling of documents, printed matter and other media, in particular visual recordings, audio recordings and audio-visual recordings that could be used to identify the natural person who provided the information to ensure that the identity of the information source is not revealed.*

While this legislation offers stronger legal protection for journalists' sources, it does not take account of the issues identified in this study pertaining to the digital era developments that may risk undermining such legislative guarantees, including data retention (see reference to Slovakian law in the relevant section above) and mass surveillance.

Iceland ratified a new law in 2011 that strengthened journalistic source protection and freedom of expression (Hirsch, 2010, Smith 2010). A new Information Act was passed in January 2013 in which source protection is emphasised. According to the Act, journalists are not authorized to name their sources without their consent or a judge's order when it comes to a criminal case (International Modern Media Institute, 2014).

In Lithuania, amendments to the Law on the Provision of Information to the Public in July 2014 limit legal coercive action to disclose sources of information. The Law requires that it must be established that the disclosure of a source is warranted by an issue of critical public importance, or the necessity to ensure the protection of constitutional rights and freedoms, before a source is forcibly revealed.

In Estonia in 2010, the Ministry of Justice introduced legal amendments to the Criminal Code, including a provision that would allow courts to jail journalists for up to five years for refusing to disclose their sources in the context of serious crimes.

France strengthened the protection of sources with a law that took effect in 2010 (LOI n° 2010-1 du 4 Janvier 2010). It stated that journalists could only be compelled to reveal sources when the information is required for the investigation of a serious crime (The Economist 2010). In March 2012, the Paris Court of Appeals rejected a case brought by Le Monde. In 2013, a new bill was mooted in the French parliament (projet de loi n° 1127,

20 The ECtHR stated that future costs order would have "no impact on public interest journalists who vehemently protect their sources yet recognise and respect the rule of law". Mahon Tribunal v Keena & anor [2009] IESC 78

déposé le 12 juin 2013) with the intention of expanding and strengthening the protection of journalistic sources (Ministry of Justice 2013). At the time of writing, it had yet to be approved (Assemblée Nationale (a): 2013) (RSF 2014a, Damge & Cosnard 2015).

In June 2010, the Supreme Court of the Russian Federation issued a clarification regarding the Law on Mass Media, stating that in a case involving the disclosure of the source of information, courts should follow part 2 article 41 of the Law of the Russian Federation on mass media under which:

> *The editorial staff is obliged to keep the source of information a secret and has no right to name the person who has provided the information on condition of non-disclosure of his [sic] name, unless the court has demanded the opposite in connection with the case being tried. […] During any stage of the deliberations the court has the right to demand corresponding editorial staff disclose the information on the source if all other means of finding the circumstances vital for the settlement of a case are exhausted, and the public interest in disclosure of the source of information outweighs the public interest in keeping it a secret* (Supreme Court of the Russian Federation: 2010).

Portugal amended its Statute of Journalists (Journalist's Statute Law no. 01/99) in late 2007. Article 11 (1) states that: "Without prejudice to the provisions established in penal procedure law, journalists are not required to reveal their information sources, and their silence thereof is not liable to any direct or indirect sanction".

In September 2014, the Dutch parliament began considering two new Bills on the protection of journalistic sources, following judgments against the Netherlands over the European Convention on Human Rights and involving cases concerning journalists and source protection. The first Bill amends the Intelligence and Security Services Act 2002 to require a binding judicial review from the Court of The Hague before intelligence and security services are allowed to apply their special powers to journalists in order to uncover their sources. This proposal addresses the main issue in the ECtHR judgment against the Netherlands in the Telegraaf Media case (see Regional Instruments section of the study) (Breemen 2014). The Bills, which were still progressing through the Dutch parliament at the time of writing, were welcomed by the Dutch journalists' union (NUJ 2014).

At the time of writing, Switzerland's *Basler Zeitung* was awaiting a decision by the European Court of Human Rights regarding its appeal against a Federal Court decision involving a journalist asked to reveal the identity of a source. The Basel Court of Appeal had rejected the State Attorney's order that the journalist reveal the identity, however, on further appeal, the Federal Court found that the crime could not be solved without the journalist identifying the source. The court also indicated than an overriding interest in publication of the article did not exist because there was no evidence of political, economic or public administration impacts (International Law Office 2014b).

In Armenia in 2014, *Hraparak* newspaper and iLur.am (an online news publisher) appealed to the Republic's highest appeal court, the Court of Cassation, against a lower court order obliging them to reveal their confidential sources in an assault case. The court of First Instance and the Court of Appeal both ruled that the two media organisations should disclose the source of their reports, upholding the prosecution's case that the protection of public interest in the criminal process was stronger than the public interest in not disclosing the source (Sayadyan 2014).

In August 2012, a district court in the Czech Republic reversed fines imposed by police on the weekly newspaper *Respekt* for refusing to reveal the source of a document related to a corruption scandal. The court found that the information was not necessary to the police investigation (Freedom House 2013b).

Israel's Knesset in 2014 discussed the possibility of introducing measures to provide greater protection for journalists who obtain national security leaks from confidential sources (Freedom House 2014g). The proposed law had not been ratified at the time of writing.

The German parliament also passed a law as an amendment to the Criminal Code and Code of Criminal Procedure in 2012. This prohibited the prosecution of journalists for reporting classified information obtained from government informants as well as prohibited searches and confiscation of journalistic material and offices in connection to the same case (IRIS 2012).

In Greece, the protection of source confidentiality is mentioned only in the Code of Ethics for Journalists that was established in 1998 by the Journalists' Union of the Athens Daily Newspapers (ESIEA). Although source protection is not established in Greek law, ESIEA's code of Ethics (article 2) refers to the journalist's rights, duties and obligations. At paragraph i) it says "The journalist is competent and obliged: To adhere to professional discretion as to the source of information which has been obtained in confidence" (ETHICNET). The code had no legal status at the time of writing.

ii. North America

The two countries in North America: The United States of America and Canada both recorded notable developments in the arena of legal protections for journalists' sources in the period 2007-2015.

Countries demonstrating changes in North America: Two out of two (100%)

- United States of America
- Canada

a. National Security/Anti-terrorism impacts

In the USA, the Government pursued eight leak-related prosecutions between 2008-2015 on national security grounds (Savage 2014a). This involved confidential journalistic communications being subpoenaed in a number of cases, and the reaction ultimately leading to a revision of procedural rules in an attempt to better protect source confidentiality. Reference to national security issues was a factor in the case discussed below.

In 2013, it was revealed that US Government officials had subpoenaed the telephone records of Associated Press (AP) reporters for a two-month period during the preceding year (Sherman, 2013; Savage & Kaufman 2013). This occurred notwithstanding the Justice Department's own guidelines (28 C.F.R. § 50.10) (Reporters Committee for Freedom of the Press, 2013). AP Chief Executive Gary Pruitt stated that the records potentially revealed communications with confidential sources across all of the company's news gathering activities during a two-month period.

Also in 2013, *Der Spiegel* reported that the NSA had intercepted, read and analysed internal communications at Al Jazeera which had been encrypted by the news organisation (Der Spiegel 2013). The story was based on reported NSA documents leaked by Edward Snowden.

The New York Times journalist James Risen faced jail for refusing to reveal a source cited in his 2006 book *State of War* after he exhausted all legal options up until a failed Supreme Court review (*United States of America v Jeffrey Alexander Sterling; James Risen* US Court of Appeals for the Fourth Circuit, No 11 – 5028, July 19 2013) (Hillebrand 2012; Warren 2014). The US Justice Department later abandoned its bid to compel Risen to reveal the source in court after outgoing US Attorney Eric Holder said that no reporter who is doing her/his job would go to jail on his watch. In January 2015, the jury convicted the accused source without Risen's testimony, referring to phone records showing that the two were frequently in contact (*The Economist* 2015). The source was ultimately jailed for three and a half years (Editorial Board, *The New York Times* 2015).

Another journalist's confidential source was jailed in the US on espionage charges, after the FBI obtained a warrant to access Fox News reporter James Rosen's phone and email records (Case 1:10-mj-00291-AK US District Court 2010). According to court documents, FBI investigators also used the security-badge data of the source, in combination with phone records and e-mail exchanges with the journalist, to build a case. They targeted the movements of the source and the journalist a few hours before the story was published in June 2009 (Marimow 2013).

Investigators reportedly needed to access the journalist's emails because they suspected that the source had deleted some from his own accounts (Savage 2014a; Case 1:10-mj-00291-AK, US District Court 2010, 11 January 2011). The law circumvented by the search warrant that allowed investigators access to Rosen's emails is U.S. Code § 2000aa 'Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses'. It stipulates that: "it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication" unless the person is reasonably suspected of being directly involved in the crime to which the materials relate. (Legal Information Institute, date unknown).

In early 2015, after a period of negotiation with US media houses, their lawyers, and press freedom groups, and in response to strong criticism, the Goverment moved to address concerns about the undermining of source protection frameworks in the context of leak investigations. It signed into force new guidelines restricting access to journalists' phone records and digital data. (See discussion in section d below).

In January 2015, journalist Barrett Brown was jailed in the US for 63 months on charges that amounted to linking to material released in connection with the hacking of a private intelligence contractor (Woolf 2015). During the trial, the FBI obtained a warrant to access Brown's laptop, with the authority to seize any information related to the group Anonymous and others. This warrant permitted access to "email, email contacts, 'chat', instant messaging logs, photographs, and correspondence" (see also Ludlow 2013).

In Canada, the Security of Canada Information Sharing Act – anti-terrorism legislation known as Bill C-51 - was passed by the parliament in June 2015 (Therrien 2015). Canadian Law professors Craig Forcese and Kent Roach have also pointed to the likely chilling effect

of the Act on freedom of expression, including journalistic communications (Forcese & Roach 2015).

b. Mass Surveillance and targeted surveillance

Confidential documents leaked by Edward Snowden, first published by the US edition of the UK newspaper *The Guardian* on June 5 2013, reported that the US National Security Agency (NSA) monitored telecommunications metadata of citizens (Bauman et al 2014; Moore 2014). Another article in early 2015 reported that the NSA and GCHQ had hacked a company that makes phone SIM cards, which could compromise the security of millions of phones around the world (Scahill 2015).

On June 2nd2015, the US Senate passed the USA Freedom Act. The Act, which supercedes the Patriot Act, ends the practice of bulk collection and storage of US citizens' metadata phone records by the NSA. It also places responsibility for storing citizens' data in the hands of private companies, mandates creation of a panel of public-interest advocates for the court that oversees surveillance programs (US Foreign Intelligence Surveillance Court, FISA) in cases that involve novel or significant legal issues, and requires the Court to notify Congress when it reinterprets law. Other surveillance powers, including email and Internet interception, remained unaffected (Siddiqui 2015, Ackerman 2015, Yuhas 2015).

In a case beginning in 2008, *The Nation Magazine* and the Pen America Centre joined an action against the head of the NSA and the US Attorney General in the District Court of New York (*Amnesty International et al V Clapper et al* 2008) alleging that their constitutional rights were being violated by electronic surveillance which undermined and obstructed their work with confidential sources. The case was dismissed because the plaintiffs could not prove that they had been subject to 'dragnet surveillance'. However, in May 2015 in the Second Circuit Court of Appeal found for the plaintiffs, declaring bulk collection of American's phone records illegal.

In 2013, US District Court Judge Richard J Leon ruled that the NSA's bulk surveillance and long-term of telephone calls violated the Fourth Amendment privacy-related protections against unreasonable searches and seizures (*Klayman v Obama Civil Act No. 13-0851(RJL)* December 1, 2013). The case was the subject of an appeal by the US Government at the time of writing.

Pro Publica and the American Civil Liberties Union have separately launched three legal challenges to secrecy surrounding NSA and Foreign Intelligence Surveillance Court processes regarding the authorisation of mass surveillance (Brandeisky 2013). The cases, all lodged in 2013, were still pending at the time of writing.

In March 2015, *The Nation Magazine*, Pen America, Wikimedia, *Amnesty International* USA, Human Rights Watch and others launched a joint action in the Maryland District Court, challenging the NSA's bulk interception and searching of Americans' Internet communications, including emails, web-browsing content, and search-engine histories (Wikimedia et al Vs NSA Case 1:15-cv-00662-RDB). (See further discussion of this case in the 'Entitlement to claim protection' section below).

In Canada in 2010, a court (see discussion re: R. v. National Post 2010 below) declared that mass surveillance undermines commitments that journalists make to protect sources (Best 2010).

c. Data retention/Third party intermediaries

The AP case cited above highlighted the issue of the retention of journalists' data, including data that may identify confidential sources, by third parties. Telecommunications carriers (phone, mobile and fixed-line broadband) companies and major Internet services are among these third parties, and US law enforcement and security officials have argued that there is no expectation of privacy for those records. The key case in this area is Smith v. Maryland, and it is under challenge by civil libertarians and others (Smith v Maryland 442 US 735 Supreme Court 1979).

The Risen case discussed earlier also shed light on the impact of data retention on reporters' dealings with confidential sources. He concluded that his travel records, credit data and phone records had been accessed (CBS 2015). Similarly, in the aforementioned Rosen case, the reporter's email correspondence and phone records were subpoenaed. There was a media outcry in response and Rosen was not prosecuted (*The Intercept* 2014).

Other cases of data retention and access took place with potential relevance to source protection. It emerged in early 2015 that Google had turned over data about Wikileaks and its staff to the US Government, under a secret search warrant that included instructions not to tell Wikileaks (Kravets 2015). The search company did not tell Wikileaks in a timely manner after it was released from the gag order. Ross La Jeunesse, Global Head of Free Expression and International Relations at Google, told the author that the company deals daily with thousands of requests for revelations and Google frequently pushes back against such requests "But we are under the law and we are forced to comply if it's been through due legal process" (Posetti 2015c).

In 2013, the US Government sought access to the encrypted email messages and metadata of a user of the Lavabit encrypted email service in the Eastern District Court of Virginia (US V Lavabit) The owner of Lavabit resisted, shut the company down and the case was under appeal in mid-2015 (Phillips M and Buchanan M 2013).

Several third party intermediaries, including Google, Microsoft, Facebook, LinkedIn and Yahoo successfully challenged a range of cases of US Government requests for their clients' data before US courts in 2013, enabling them to make limited revelations. (c.f. Brandeisky 2013). These judgements served to increase a degree of transparency around such requests.

In 2011 and 2013, the Electronic Frontier Foundation brought actions on behalf of two unnamed telecommunications companies who challenged the legitimacy of so-called National Security Letters. These US Federal Bureau of Investigation (FBI) 'letters' make it illegal to disclose information about US Government demands for citizens' phone records. A Federal judge ruled in favour of the plaintiff in one case on the grounds that the 'letters' were unconstitutional and ordered the FBI to stop producing them (US District Court 2013). However, he found against the plaintiff in the second case (US District Court 2013b) and the US Government was in the process of appealing the first decision at the time of writing.

d. Entitlement to Protection: Who is a journalist? What is journalism?

At the time of writing, the US was debating a proposed federal shield law in the Senate (*Free Flow of Information Act of 2013*). The definition of "journalist" under the Bill includes someone who was an "employee, independent contractor or agent of an entity or service"

who, among other things, "disseminates news or information by means of newspaper… news website, mobile application or other news or information service (whether distributed digitally or otherwise)" (*Free Flow of Information Act of 2013*, s11(1)(a)i)(I) 'Covered journalist'). The section also defines journalism methods, such as "collecting interviews". (*Free Flow of Information Act of 2013*, s11 (1)(a)i)(I) 'Covered journalist'). The bill had not become law by the time of this Study's conclusion in July 2015 and it is uncertain whether it would extend to bloggers doing journalism.

In some US states, such as California (Cf O'Grady v. Superior Court, 139 Cal. App.4th 1423), legislatures and courts have explicitly extended the protection to non-traditional journalists operating as online news producers.

Canadian courts have also discussed the issue in case law. The Canadian Supreme Court justices, referring to the precedent *Grant v. Torstar Corp., 2009 SCC 61, [2009] 3 S.C.R. 640*, stated that law enforcement would be weakened if source protection was not limited to the traditional media (*R. v. National Post*, 2010 SCC 16, [2010] 1 at para 40).

e. Other digital dimensions

In one reported case, police searched the home of a Journal de Montréal reporter, taking his computer (RSF 2012). This example is not provided with the presumption that confidential journalistic data was unduly exposed.

f. Anonymity issues

No additional developments were recorded during the research period.

g. Other dimensions

As indicated above, at the time of writing, the US was debating the introduction of a federal shield law. This was against the backdrop of fragmented and differing shield laws found at state level, which has highlighted a need for a consistent application of shield law protections at federal level for US journalists. According to the Reporters Committee For Freedom of the Press, 36 states plus the District of Columbia now have a journalists' "privilege" (Ruane 2011) in their laws or rules (with Utah and New Mexico recognising the privilege through court-adopted rules). All of the other states — apart from Wyoming — have court decisions recognising some level of special protection (Leslie, 2008).

The disparity of state shield laws was illustrated when the accused in a court case attempted in 2013 to compel a New-York-based Fox News journalist to reveal her confidential source. However, an appeal court found that Jana Winter was protected under New York's shield laws from revealing her source, and she was not subject to the weaker Colorado laws (*In the Matter of James Holmes v. Winter, ___ N.E.2d ___, 2013 WL* 6410422, 2013 N.Y. Slip Op. 08194 at 23, 25 (Dec. 10, 2013).)

As discussed earlier in this Study, the US Government has been criticised in connection with actions designed to discover journalists' sources, in the course of leak investigations (Savage 2014b). In response to these concerns, the US Government embarked upon a series of high-level consultations with media industry representatives, advocates, academics and press freedom organisations. Following these consultations, the US Department of

Justice published the *Report on News Media Policies* in July 2013 which carried a preamble describing revisions designed to "strike the proper balance among several vital interests," such as protecting national security and "safeguarding the essential role of the free press in fostering government accountability and an open society" and contained recommendations for renovating procedures (DOJ 2013). The recommendations included:

i. Reversing the Existing Presumption Regarding Advance Notice

This new rule requires authorities to notify news media in advance when access to their communications records is sought, in all but the most exceptional cases.

ii. Enhanced Approvals for Use of Search Warrants and Section 2703 (d) Orders

This rule limits the power to over-ride the journalistic materials seizure exception by stipulating that it can be circumvented only when the member of the news media is the subject of a criminal investigation for conduct not connected to ordinary newsgathering activities. Secondly, the rule requires applicants for search and seizure warrants pertaining to news media activities to establish that such access is essential and that permissions are narrowly framed to ensure that only material necessary for the investigation is targeted.

iii. Establishment of a News Media Review Committee

This Committee (comprised of experts within the Justice Department who are not involved in the cases under consideration) is established to advise the Attorney General when Departmental officers request: a) access to news media records in leak investigations; b) authority to access the reporting records of a member of the news media without prior notice; c) testimony from a member of the news media that would expose a confidential source.

iv. Centralisation of Review and Public Reporting Requirements

This provision is designed to enhance oversight and tracking of the outcome of DOJ requests for news media subpoenas.

v. Intelligence Community Certification

This certification process is designed to ensure that requests for access to news media records in the case of investigations connected to revelations of classified or national security-related information are proportionate.

vi. Safeguarding information

This clause promises a revision of the safeguards regarding proper use and handling of the communications records of members of the news media. It intends to ensure that records obtained are kept secure, while limiting access, usage and sharing of the data.

vii. Technical Revisions

With significance for this study, this point acknowledges the need to account for technological changes in newsgathering, distribution and publication. It extends the rules above to the records of news media members that are held by third party intermediaries.

viii. Written Guidance and Training Requirements

This point highlights the need to ensure that law enforcement officers and relevant Department officials are educated about the above changes and equipped to implement them.

ix. Establishment of a News Media Dialogue Group

The value of stakeholder engagement in regulating access to private news media communications is recognised here. The Group is described as having representatives from the news media, the DOJ and its Director of Public Affairs.

x. Intelligence Agency Administrative Remedies

This point provides guidelines for investigating leaks designed to internalise enquiries to limit impacts on the news media.

Following up on these recommendations, the USA's Attorney General signed off on a new set of Department of Justice guidelines in February 2014. Titled *Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting or Charging Members of the News Media*, the new rules (DOJ 2014) include the presumption that news media will receive advance notice from prosecutors when attempts are made to access their journalistic communications. They also further limit exceptions to a law forbidding search warrants for journalistic material unless they are suspected of criminal activity, stating that warrants cannot be invoked in the context of ordinary newsgathering activities. The new rules apply to criminal investigations, and exempt wiretap and search warrants obtained under the Foreign Intelligence Surveillance Act (FISA) as well as subpoenas used to obtain records about communications in terrorism and counter espionage investigations on national security grounds.

In Canada, in 2010, a reporter in possession of documents alleging the fraudulent conduct of a third party successfully had search warrants set aside, after he claimed that he obtained them from a confidential source (*R. v. National Post*, 2010 SCC 16, [2010] 1). However, the Canadian Supreme Court rejected the reporter's claim to a constitutional right to shield the identity of sources during criminal investigations, instead favouring deciding the issues on a case-by-case basis. In considering the appeal, the Court relied on the Wigmore Criteria to determine that the journalist in the case could not claim a right to source protection (2010 SCC 16). John Henry Wigmore was an expert on evidence law (Best 2010) who developed these criteria in his influential "Treatise on the Anglo-American System of Evidence in Trials at Common Law" (Wigmore 1923). Wigmore suggested that confidentiality would be upheld if the following criteria were met:

1. The communication originates in a confidence that it will not be disclosed…;
2. The confidence must be essential to the relationship in which the communication arises;
3. The relationship must be one which should be "sedulously[21] fostered" in the public good. And (if all of the criteria 1-3 have been satisfied) then;

21 ("Sedulous[ly]" being defined in the New Shorter Oxford English Dictionary on Historical Principles (6th ed. 2007), vol. 2, at p. 2755, as "diligent[ly] . . . deliberately and consciously". R. v. National Post [2010] 1 SCR 477, at para [53]

4. The court must consider whether in the instant case the public interest served by protecting the identity of the informant from disclosure outweighs the public interest in getting at the truth

The judges concluded by majority opinion that:

> *The bottom line is that no journalist can give a source a total assurance of confidentiality. All such arrangements necessarily carry an element of risk that the source's identity will eventually be revealed. In the end, the extent of the risk will only become apparent when all the circumstances in existence at the time the claim for privilege is asserted are known and can be weighed up in the balance. What this means, amongst other things, is that a source who uses anonymity to put information into the public domain maliciously may not in the end avoid a measure of accountability (2010 SCC 16: 69)*

Also in Canada, in 2012 three cases emerged involving attempts to compel journalists to reveal their sources or the use of search warrants to discover them. In the first case, a Quebec judge ordered a journalist from the news website MediaSud to reveal his sources for a story on the leak of a confidential report to another journalist. In the second case, a Quebec court ruled against an attempt by a real estate developer to get a Radio-Canada reporter to reveal his source.

Regional Conclusion

25 out of 38 (66%) of countries examined in the UNESCO region of Europe and North America experienced significant developments pertaining to source protection laws in the period 2007-2015. These changes reflected the key themes identified in this report associated with emerging digital effects on legal source protection frameworks: a) national security/anti-terrorism impacts; b) Surveillance; c) Data retention/handover and the role of third party intermediaries; d) Questions about entitlement to claim source protection; e) Increased risk of source exposure due to digitally stored journalistic communications being seized during investigations.

6.5. Latin America and The Caribbean

> *The recognition of protection of journalistic sources is generally respected in Latin America both at the regional and local levels. Most countries have adopted constitutional or legal protections which give a strong level of legal protection. …There are also important declarations from the Organization of American States. Few journalists have been forced to reveal their sources by courts, however direct demands for sources still occur regularly in many countries, requiring journalists to seek legal recourse in courts. There are also problems with searches of newsrooms and journalists' homes, surveillance and the use of national security laws. (Banisar, 2007: 81)*

Between 2007-2015, a number of developments in Latin America have had an actual or potential bearing on source protection, including mass surveillance, national security legislation, searches of newsrooms and journalists' homes, and physical threats.

At the individual States level, developments in regard to source protection coverage 2007-2015 were identified in 17 of the 20 countries (85%) examined in Latin America and the Caribbean – all of these countries are in Latin America:

- Argentina
- Bolivia
- Brazil
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Ecuador
- El Salvador
- Guatemala
- Honduras
- Mexico
- Panama
- Paraguay
- Peru
- Uruguay
- Venezuela (Bolivarian Republic of)

According to the Editor-in-Chief of Argentina's La Nacion, Carlos Guyot, who spoke to this study's research team, in Latin America the laws are strong in many settings but enforcement is weak (Guyot 2015). In addition, while many countries have laws in place to protect journalists' sources, it is increasingly evident that sources can be identified by other means such as intercepts, threats, searches, accessing stored data, and biometrics. These factors, along with the classification and restriction of information in the name of national security, have relevance to whether protections for journalists' sources are substantively effective.

Surveillance was a theme in ten of the countries studied, five of which (Bolivia, Ecuador, Colombia, Paraguay, Mexico) introduced new laws that allow data retention and/or interception during the period examined. Four countries (Peru, Honduras, Panama, Costa Rica) have proposed variations to state secret laws or information classification laws which, in some cases, allow for prison sentences, for revealing such information. Three countries in the region introduced new source protection dispensations, including the one enshrined in the 2010 Constitution of the Dominican Republic.

a. National Security/Anti-terrorism impacts

Overly broad regulations instituted in the name of national security and anti-terrorism measures may be seen to pose a risk to journalistic source protection in parts of Latin America.

Peru's Decree No. 1129 classifies all information related to national security and defence as a state secret (Article 12). It imposes a punishment of up to 15 years in prison for those who reveal such information. According to the Inter American Press Association (IAPA 2013), the Decree states that: "any person who by reason of his or her position or function, becomes aware of classified information of a secret, reserved, or confidential nature, related to Security and National Defence, is obliged to keep the corresponding secrecy". The Computer Crimes Law enacted in 2013 penalizes the release of classified or secret information that compromises national defence security with five to 10 years in prison (Khan, 2013). In February 2013, the Ombudsman's Office of Peru filed an action of unconstitutionality against Article 12 of the Decree, arguing that it violated the right to access public information because: "The article establishes the secret nature of all documentation or information regarding matters referring to national security and defense, along with the obligation of every person to maintain secret all information on such matters in their possession" (Botero 2013; IPYS/IFEX 2012; OSF 2014c). The outcome of this action was unknown by mid-2015 when the research for this study was concluded.

In January 2014, the Honduran parliament approved the Official Secrets Law, which was then suspended pending further study. The law gives state entities the power to classify information from "restricted" to "ultra-secret". In Article 13, those with access to classified information are warned that revealing it leads to sanctions (Griffen 2014).

El Salvador's Public Access to Information Law (LAIP), first passed in 2010, also includes a classification of information as military secrets and data compromising national security. The classification allows for formal punishments for accessing or revealing such information, even if it is in the public interest (Bachmann 2010). Also in 2010, the Legislative Assembly introduced a motion to subject staffers to a polygraph test in order to identify an individual who had leaked information to the media concerning salaries for legislators. However, this initiative was withdrawn due to public opposition (Freedom House 2011c).

Venezuela saw the introduction of the Strategic Centre of Security and Protection of the Homeland (Decree CESPPA), which has a wide mandate to monitor all online communications (El Nacional, 2014).

In Panama, an Information Security Bill, which would have imposed prison sentences for those who gained access to classified information and publicised it (Article 429) was withdrawn in 2012 (Higuera 2012, Simmons 2012).

In Costa Rica, the government announced that the Cybercrime Offense Law 9048 2012 - which imposes one to six years in prison for revealing state secrets related to national security, defence of sovereignty and foreign relations – would not apply to journalists (RSF 2013a, RSF/IFEX, 2012). In April 2013, the National Assembly revised the legislation and eliminated Article 288 which would have imposed a prison sentence with up to 10 years in jail for releasing "state secrets". The revisions also removed prison terms in the case of protected information released in the public interest (Freedom House 2014h)

b. Mass Surveillance and targeted surveillance

In Columbia, *La Semana* magazine revealed that the Colombia Administrative Department (DAS) reportedly conducted illegal surveillance over six years, including on the telephones and emails of journalists, NGO workers, supreme court justices, politicians and government critics from 2007-2009 (Soendergaard, 2014). After the dismantling of the DAS, the former head of the Department, Maria del Pilar Hurtado, was convicted of illegally spying on human rights activists, journalists, politicians and judges. She was sentenced to 14 years jail in May 2015. In the same case, the high court also sentenced Bernardo Moreno, a former senior official, to eight years under house arrest after he faced charges including unlawful violation of communications (*Latin American Herald Tribune* 2015, Botero 2015).

In 2014, Colombian military intelligence reportedly intercepted around 2,600 emails between Revolutionary Armed Forces of Colombia (FARC) spokespeople and international journalists during peace negotiations (Cruz 2014, AP 2014, *Panam Post* 2014). Colombia-based Foundation for Freedom of the Press (FLIP) official Pedro Vaca Villareal told this study's researchers that surveillance in Colombia is founded on the Law of Intelligence (Law 1621 of 2013) and the Law of Public Security (Law 1453 of 2011). These allow the monitoring of the electromagnetic spectrum and access to subscriber data from telephone companies.

In 2009, Peru's former President Alberto Fujimori was sentenced to six years in prison for the wiretapping of journalists, politicians and businessmen during his term (Lauría 2010). The following year, a former naval intelligence employee was revealed to have reportedly intercepted 52,947 emails of journalists and political opponents during the Fujimori government (Rodriguez, 2011).

In 2011, it was revealed that Peru's Congress had reportedly covertly investigated telephone calls made by a group of journalists who had alleged corruption by government officials (Cruz 2011). In the aftermath of a court case, the Supreme Court of Peru proposed prison sentences for those who publish private communications obtained by illegal wiretapping (Medel 2011 b; Peru21, 2011). Also in Peru, a journalist who specialised in reporting drug trafficking and terrorism was interrogated about his sources, based on wiretaps used by intelligence units against terrorist groups, the Inter-American Commission of Human Rights reported in 2013 (Botero 2013).

Concerning Brazil, the Director of the Institute for Technology and Society of Rio De Janeiro, Professor Ronaldo Lemos told this study that large companies and the Brazilian Presidency had been the targets of surveillance programs. "Accordingly, journalists working with sources connected with these institutions might have been collaterally affected," he said (Lemos 2015). According to World Editors Forum Chairperson, and Executive Director of Journalism at Grupo RBS, Marcelo Rech, targeted surveillance connected to police investigations into organised crime and corruption is a problem for journalists dealing with confidential sources in Brazil. Rech identified a case in November 2014, in which a prosecutor asked that a judge waive the confidentiality of the telephone lines and the mobile lines of the newspaper *Diário da Região*, in order to identify the source of a story about corruption. The judge issued the order but the newspaper and the national Brazilian newspaper association asked for the Supreme Court to suspend the order. In January 2015 the Court suspended the order on the basis of its unconstitutionality (Rech 2015).

The Supreme Court of Costa Rica ruled in 2014 that government surveillance of phone records of *Diario Extra* journalist, Manuel Estrada, was unconstitutional (IPI 2014a). The court found that the surveillance violated the privacy of the reporter and it ordered the

investigative agency to destroy all recordings pertaining to the investigation, while prohibiting any government agency from carrying out this type of operation in the future. The judge also criticised the prosecutor's office for authorising the operation (IPI 2014a).

New Laws Permitting Interception

In Bolivia, the 2011 *Telecommunications, Information Technology and Communication Law* permits telecommunications interception in cases of danger to state security, external threat, and internal shock or disaster (Article 111). Under this law, telecommunication providers are obliged to cooperate with authorities when asked to provide information (Lara 2011) .

In Ecuador, Article 14 of the 2012 *Telecommunication Service Subscribers and Added Value Registration Act* prohibits third party interception of communications, however, Article 29.9 of the same resolution allows the regulator CONATEL to track IP addresses from ISP customers without judicial order (Freedom House 2013d). A similar clause appears in the Peruvian Computer Crimes law that also allows police to access users' personal information without a court order.

c. Data retention/Third party intermediaries

Article 1 of Colombia's *Decree 1704* of 2012 on communications interception and data retention states: "The interception of communications, regardless of the origin or underlying technology, is a public security mechanism that seeks to optimize the investigation of crimes that is conducted by competent authorities and agencies, within the framework of the Constitution and the Law" (EFF 2012). Decree 1704 also compels Telecommunication Service Providers including ISPs to implement technological means and infrastructure that accommodate access to the networks by judicial police (EFF 2012).

Further, Article 4 requires that communications providers must retain and store subscribers' personal information for five years. Once the relevant legal requirements have been met, telecommunications network and service providers must deliver to the authorities the subscriber's data such as identity, invoicing address and type of connection.

Signed into law in 2014, Mexico's *Broadcasting and Telecommunications Act* requires providers to store data from clients in Mexico and grants national security agencies and police access to this data in the name of national security (IPI 2014c). Article 190 states an obligation to retain data for 24 months (Ley de Telecomunicaciones y Radiodifusión 2014). Former Special Rapporteur on Freedom of Expression at the Inter-American Commission on Human Rights Catalina Botero reported to this study's researchers that the law covers metadata and geolocation information, and that it allows the authorities to access the data without a court order.

Article 474 of Ecuador's *2013 Organic Penal Code* requires that ISPs store user data in order for the state to carry out corresponding investigations (Lavin & Betancourt 2013).

Paraguay's 2014 Data Retention Bill obliges service providers and hosting service providers to store data for a minimum of six months (Lexology 2014).

Argentina's proposed data retention law (National Telecommunications Law of 2003 Amendment) was ruled unconstitutional in 2009. It would have required all telecommunications companies to store data for 10 years (EFF 2009).

In Brazil, the Internet Bill of Rights' sections on privacy and data retention (Articles 13 and 15) require Internet access providers and Internet service provides to retain data for one year and six months, respectively. Regulation of such provisions was still pending at the time of writing (Law No. 12.965 of 23 April 2014).

d. Entitlement to protection: Who is a journalist/What is journalism?

The issue of entitlement to claim source confidentiality privileges was raised in 2014, when the Supreme Court of Costa Rica ruled on government surveillance of *Diario Extra* journalist, Manuel Estrada (noted above). Presiding Judge Ernesto Jinesta Lobo also referred to people who regularly contribute to reporting or public opinion as a category outside traditionally defined reporters to whom protection from surveillance applies (IPI 2014b).

Legislative changes regarding the definition of 'professional journalists' in the Ecuador Communications Act attracted the concern of the Inter-American Commission on Human Rights' Annual Report in 2013. The Act establishes that only professional journalists and media workers may perform journalistic activities of the media, at any level or position. Exceptions are made for those who have specialized knowledge, or opinion-based programs and columns, and those who perform journalistic activities in the languages of the Indigenous peoples and nations (Art. 42) (Botero 2013: 148).

Mexico City (a federal entity within Mexico) has the *Professional Secrets of Journalists Law* which defines "journalists" as "Individuals as well as media and public dissemination, community, private, independent, college, experimental" and extends to "or any other whose job is to collect, generate, process, edit, comment, review, disseminate, publish or provide information through any media and communication that can be print, radio, digital, or image, permanently, with or without compensation and without professional qualification or registration required" (Article 1).

The 'Who is a journalist?/What is journalism?' issue has also been debated in the Dominican Republic, where a proposed law would criminalise the practice of journalism without a journalism degree from an accredited school of journalism or communications. Punishment would include up to two years in jail and a US$25,000 fine (Lara 2012c). In 2012 the university degree requirement for journalists also existed in Bolivia, Cuba, Chile, Honduras and Nicaragua.

In 2009, the Brazilian Supreme Court ruled that a journalism degree was not mandatory for the exercise of journalism in that country (Supremo Tribuno Federal, 2009).

e. Anonymity issues

The Brazilian Constitution states that "access to information is ensured to everyone and the confidentiality of the source shall be safeguarded, whenever necessary to the professional activity". Anonymity is forbidden in all other circumstances. This provision has recently been interpreted by courts and Public Prosecutors (Ministério Público) as a means to ban apps and software that provide anonymity on the Internet. Such case law is still recent (Nelson, Mashable 2014), but if confirmed over time, it could lead to restrictions on the availability of relevant tools for journalists to communicate with anonymous sources.

f. Other digital developments

Chile passed a Net Neutrality law prohibiting ISPs to arbitrarily block, interfere, discriminate, hinder or restrict legal content that users send, receive or provide via the Internet (Ley 20453 2010; Ruiz 2010).

g. Other dimensions

Since Mexico's introduction of a federal shield law in 2006 (Banisar 2007:83), three states have introduced protection for journalists' sources. As signalled above, Mexico City has the *Professional Secrets of Journalists Law* which states in Article 1 that journalists are entitled to keep secret the identity of sources who have provided information (Noticeros Televisa 2014). Additionally, another shield law has been passed in Chihuahua (Medel, 2011), while a bill was introduced in Coahuila (Harlow, 2010).

In Ecuador, the new Organic Communications Law (2013) guarantees the right of journalists not to go against their beliefs, to protect their sources, and their right to professional confidentiality (RSF 2013b, Martínez 2013).

The Dominican Republic, which previously had no laws for source protection (Banisar 2007: 85), introduced a new constitution in 2010, including two clauses acknowledging the protection of confidential sources:

> *Article 70: Habeas data: Every person has the right to a judicial action to know of the existence and to access the data corresponding to them that is found in registries or public or private data banks and, if case of falsehood or discrimination, to require its suspension, rectification, updating and confidentiality, in accordance with the law. The secrecy of the sources of journalistic information cannot be affected.*
>
> *Article 49: Freedom of expression and information: The professional secret and the clause of conscience of the journalist are protected by the Constitution and the law* (Constitute Project 2010)

In Brazil, the renovation of freedom of expression-related legal frameworks has resulted in significant impacts on the activities of journalists and the protection of sources. The Press Law from 1967 was revoked in 2009, but in the process so was this provision: "No journalist or radio commentator nor, in general, any person mentioned in Article 25 shall be compelled or required to give the name of his informant or news source, and his silence in this regard may not make him liable directly or indirectly to any kind of punishment" (Article 71).

In Argentina in 2014, police searched the radio station La Brújula 24 under a court order with the aim of pursuing the identity of the source who leaked government wiretap recordings to the station (CPJ 2014a). The case was still under investigation at time of writing.

In the Dominican Republic in 2012, investigative reporter Nuria Piera published a story titled *The Route to Millions* (Investigacion Periodistica 2012) in which she wrote about political funding. Piera reported that state intelligence officers searched her home and office in pursuit of her story's sources (Lara 2012a; Free Media 2012)

In Panama in 2013, the Attorney General's Office announced the intention to carry out inspections and gain access to journalists' equipment at newspapers *La Estrella* and *El Siglo* with the intention to discover the source/s of journalists' reports. However, the Attorney

General's office withdrew approval to search the two newsrooms on the basis of Article 21 of the Law of Journalism which states: "Journalists shall not be required to reveal sources of information and origins of news, without prejudice of other liabilities they may incur". The Declaration of Chapultepec was also cited (see earlier discussion about the Declaration in Section 6.2) (IAPA 2013).

A noteworthy court ruling in terms of source protection occurred in Bolivia in 2014, where *La Razón's* Ricardo Aguilar and Claudia Benavente were accused of revealing state secrets (Knight Centre 2014). A court ordered Aguilar to reveal his sources but he told this study that he had promised his source that he would never reveal their identity and therefore he refused to do so (Aguilar 2014). Ultimately, a La Paz court ruled that the case against Aguilar and Benavente should be heard by a press court, not a criminal court. However, at the time of writing, the case had still not been before the press court.

In a landmark ruling in 2009, the Constitutional Court of Colombia protected the right to confidential sources in judgment T-298/09, in a case involving el *Diario del Huila* where a politician tried to uncover the source of a story. The Court denied the claims, upholding the inviolability of professional privilege. It also quoted verbatim Principle 8 of the Declaration of Principles, according to which: "confidentiality is an essential element in the undertaking of journalistic work and in the role conferred upon journalism by society to report on matters of public interest" (Botero, 2012: 197).

In Uruguay in 2014, a judge asked journalist Roger Rodríguez to identify his source of information regarding a case of human rights violations (*El Espectador* 2014). Rodríguez refused, and the judge did not press the issue (IAPA 2014). The same year, a Mercedes court called five journalists from the Agesor news agency to testify in a case of alleged sexual abuse at a military encampment in 2013. They were asked to reveal their sources, however they also refused (IAPA 2014).

In Guatemala in 2013, *La Hora* reported that a journalist was summoned to reveal her source before the International Commission Against Impunity in Guatemala (CICIG) and the Public Prosecutors Office, in order to discover the source of a leaked confidential report on conditions within Guatemalan prisons (Lara, 2013a).

In Peru in 2013, the Attorney General called for a journalist from *La Región* to reveal the source of his report regarding a police action (Higuera 2013).

According to information received by the Inter-American Commission on Human Rights, in 2013 in the Argentinean state of Zulia, the Scientific Criminal and Forensic Investigation Corps (CICPC) subpoenaed and interrogated a journalist with the newspaper *La Verdad* and correspondent with the organization IPYS Venezuela (La Verdad 2013; Lara 2013b, Botero 2013)

Also in Argentina, in 2011 a judge subpoenaed six newspapers for the names and office contact details of all reporters and editors who had covered Argentina's economy over the previous five years, in order to call them as witnesses in cases against their sources (AP 2011).

In Mexico, journalist Juan Carlos Flores Haro said he was held at the municipal building in San Blas and interrogated for an hour to reveal his source (Lara 2012b).

Regional conclusion

Since 2007, there have been developments in Latin America with relevance to legal source protection frameworks. These have occurred in the context of both traditional contests over the protection of confidentiality of journalistic sources, and the digital revolution which has seen an accumulation of challenges - in the form of mass surveillance and targeted interception, data retention, national security and anti-terrorism measures that can mpact on legal source protection. Additionally, questions have centred on which journalistic actors are entitled to claim coverage under source protection laws. Journalists in the region also face the conundrum that while there has been significant progress in legislation and judicidial precedents, these do not necessarily translate as tangible protections.

7. Thematic Studies

Three thematic studies were identified in the course of research for this Study to allow in-depth analysis of key issues. The thematic studies featured in this section are:

a. The impact of source protection erosion in the digital era on the practice of investigative journalism globally

b. Sweden: How a State with one of the oldest and constitutional legal source protection frameworks is responding and adapting to emerging digital transformation and associated threats

c. Model assessment tool for international legal source protection frameworks

Thematic Study 1: The impact of source protection erosion in the digital era on the practice of investigative journalism globally

This thematic study examines the practical difficulties being confronted by investigative journalists with regard to source protection in the digital age, and the significant ways in which they are changing their practices in response (C.f HRW 2014).

For this case study, qualitative research interviews were conducted with 27 investigative journalists, editors, legal experts, and freedom of expression specialists drawn from 17 countries, reflecting the UNESCO groupings of Africa, the Arab States, Asia and the Pacific, Europe and North America, and Latin America. The interviews were conducted between November 2014 and February 2015 - face-to-face, by phone, Skype and email. The quotations below are not intended to represent a scientific sample of a wider set of views, but have instead been extrapolated for the purpose of signalling the more general issues at stake. Unless otherwise indicated, the individuals cited below were interviewed as part of the research for this study.

Research context

Two recent studies have indicated the significant impact of source protection erosion on investigative journalism practices in at least one part of the world:

In February 2015, the Pew Research Center released the results of a survey on "Perceptions of vulnerability and changes in behaviour" among members of the USA-based organisation Investigative Reporters and Editors (Holcomb, Mitchell & Page 2015). Pew's research found that 64% of investigative journalists surveyed believed that the US Government collected data about their communications. The figure rose to 71% among national political reporters and those who report foreign affairs and national security issues. Ninety percent of the of US investigative journalists who responded to the Pew survey believed that their ISP would routinely share their data with the NSA, while more than 70% reported that they had little confidence in ISPs' ability to protect their data.

As a result, 49% of respondents said that over the previous year they had changed the way they stored and shared sensitive documents. Twenty-nine percent said that they had changed the way that they communicated with journalists and other editors. (See further discussion of this research under the headings 'surveillance' and 'third party intermediaries'

below, and separate research on the theme conducted for this study which is presented in Thematic Study 3).

Another study for USA-based Human Rights Watch interviewed 46 senior national security journalists from major USA news organisations, revealing the steps being taken to keep communications, sources and other confidential information secure in light of surveillance revelations (HRW 2014a: 30).

That study concluded that in the USA the combination of increased surveillance and government prosecution of leaks was having a big effect on the news gathering practices of national security reporters and their news organisations. It found that: "Journalists are struggling harder than ever before to protect their sources, and sources are more reluctant to speak. This environment makes reporting both slower and less fruitful" (HRW 2014a: 22).

The Pew study found that 45% of respondents ranked surveillance as the number one or number two challenge facing journalists (Holcomb, Mitchell & Page 2015). Nearly half of the national security, political and foreign affairs reporters among them also reported that concerns about surveillance have caused them to change the ways in which they communicated with sources (with reverting to face-to-face meetings being the main means of protecting sources). Meanwhile, 18 percent of this group reported that it was becoming harder to get sources to speak "off record".

Balancing the benefits and threats of technological change for investigative journalism in the context of source protection

a. Opportunities and threats

"Technology is allowing information to be leaked on a vast scale, a scale that couldn't possibly have been imagined…for me as a journalist we're in boom times, because you're able to get information that's incredibly detailed and you're able to get stories that you couldn't possibly [get before]", Director of the International Consortium of Investigative Journalists (ICIJ) Gerard Ryle said, declaring the digital era a "Golden Age for journalism".

Founder of the Arabic Media Internet Network, Daoud Kuttab, echoed Ryle's view of the digital era:

> *On the one hand I think it has accelerated and widened the amount of data available to everyone and made it very easy to transfer information and documents. But at the same time governments are able to invade your privacy much easier and get information.* (Daoud 2015)

Editor-in-Chief of Argentina's *La Nacion*, Carlos Guyot, also acknowledged the significant benefits of digital era investigative reporting involving confidential sources, including access to leaked documents that would have been impossible to get even five or ten years ago, although he added a caveat:

> *New technologies bring new challenges with them, but also new opportunities, like encrypted conversations via new software, although this must be combined with old fashioned practices…There is nothing like a face to face meeting with a source. …Our main investigative reporter drove for three hours to a different city for a 15 minutes conversation with a source and drove back to our newsroom. If we are willing to endure the challenges, we can still do good journalism.* (Guyot 2015)

b. Confidence of investigative journalists in legal source protection in 2015

Bolivian investigative journalist Ricardo Aguilar expressed serious concern about the reliability of legal source protection in the digital era. "…Mass surveillance, data retention and the appeal of the 'National Security' category leaves the protection of secret sources in latent vulnerability," he said.

ICIJ's Ryle said: "As a general rule these days, much more than in the past, it's very difficult to protect sources because of the fact that electronic communications can be back-tracked and people can be found much easier than they may have been found in the past…"

Executive Editor of the *Washington Post*, Martin Baron, told this study that concern about surveillance of newspapers' internal communications led to significant changes to newsroom practices during *The Post's* coverage of the Snowden story: "I didn't expect that we would have to be communicating with each other in an encrypted fashion and yet on many occasions we did just that. And on many occasions when we had meetings everybody turned off their cellphone, or left their cell phones behind..." (Baron 2015).

Director of the investigative unit at Sweden's national public radio (SR), Fredrik Laurin, was concerned about the risk of police seizing digital content due to gaps in source protection legislation in his country, and he described undertaking extraordinary digital security measures to comply with Sweden's strict laws requiring journalists to protect their sources (see Case Study 2).

But Marites Danguilan-Vitug, a co-founder of the Philippines Centre for Investigative Journalism, was more optimistic about source security. "My colleagues and I have not yet reached the stage when we're insecure about using confidential sources. Trust is still the biggest factor in keeping our confidential sources".

c. Chilling effect on sources

Co-founder of Pakistan's Centre for Investigative Reporting, Umar Cheema told researchers that the threat of surveillance is having a major chilling effect on sources. "Certainly, source insecurity is a major challenge and it is mostly [connected] with the stories about national security and high-profile government figures. It is hindering information," he said. Cheema said he believed that his status guaranteed that he is under surveillance and that his sources know it. He said that some sources approached him in the belief that he is the right person to be taken into confidence, while others hesitated because they feared that he was under surveillance and that "any contact with me will put them on radar screen".

Former Editor-in-Chief of *The Guardian*, Alan Rusbridger, told this study that the increased risk of exposure is having a direct impact on the willingness of confidential sources to share information with journalists. It had led to "a massive drying up of people willing to take the risk of talking to news organisations," he said.

ICIJ's Ryle said there is certainly increasing awareness among his sources that the stakes are much higher in the age of surveillance: "People are increasingly nervous because the truth is it's quite easy to trace people and to trace sources". International Editor of Algeria's *El Watan* newspaper, Zine Cherfaoui, said that sources are more reluctant to speak and increasingly require face-to-face meetings. "To really discuss with people we prefer to avoid electronic means or social networks. The Snowden Affair turned upside down the work of journalists… It's harder to speak to people. We really have to go out and meet them. It's face to face".

In Bolivia, *La Razon's* Ricardo Aguilar reported that sources have adjusted their behaviour, having "…intensified precautions ranging from avoiding using the phone to talk to me to not exchanging any form of correspondence, or digital messaging". However he said that there is no evidence that his sources are more reluctant to provide information. "In that sense, it seems that in the cases where I've had the opportunity to work with confidential sources, the digital age has nothing to do with the "chilling effect" because it existed by itself beyond the control of the Internet".

d. Chilling effect on journalism

The cost of digital security technology, training and legal fees in relation to digital issues is having a chilling effect on investigative journalism in some cases. Alan Rusbridger said *The Guardian* spent about a million pounds more a year on legal fees than they did five years ago, which reduces the budget to do reporting. This covered companies wanting the return of documents, who cited data protection laws and privacy, "so the bills on these things just mount and mount and mount and mount, so you can easily be spending tens or hundreds, hundreds of thousands of pounds trying to get a story into the paper," he said. "And of course once you get onto secure reporting there is a significant cost in equipment, in software, in training - particularly in trying to create a safe environment where we feel we can offer our sources the kind of protection that they deserve".

Some journalists feel they need to erase archival material to avoid it being seized. UK QC and Chair of the Centre for Investigative Journalism at Goldsmith's University, Gavin Millar, said journalists have destroyed unused content (such as un-aired interview footage) because of concerns about needing to protect their sources. He referred to the alternative being high legal costs for formally attempting to prevent the authorities from accessing un-broadcast content, for example.

Rusbridger said that communicating with sources is certainly harder now. "I think reporting just becomes much more difficult, it's much more difficult to talk to police people". He said it was also more difficult, if not impossible, to speak to municipal officials who believed their telephone lines were bugged. "All kinds of reporting are becoming much more difficult and more expensive…and time consuming".

However, in some cases, the biggest chilling effect on investigative journalism based on confidential sources is often not digital exposure of sources, but fear of subsequent consequences such as prison and death. Executive Director of the Arab Reporters for Investigative Journalism (ARIJ) Rana Sabbagh said that ARIJ has compiled 255 investigative reports over the past seven years, in many countries:

> *Not once were we asked to reveal a source... We are extremely careful and most of our stories so far haven't been the "sexy" investigations on high power or corruption. Our journalists don't have the tools to conduct such investigations, and working on these stories will either get them killed or jailed, and I don't think it's a risk worth taking. … That doesn't mean we haven't pursued big political investigations but we do a risk assessment as part of our manual and code of ethics.*

e. Changing practices

i. Journalists assume they are being watched

"I'm more careful with any digital platform that I'm involved in – whether it's email, phone or any other digital format. I assume that [I am] probably being watched, listened to, or read. That's my starting point and I take it from there," Jordan's Daoud Kuttab told this study. ICIJ's Gerard Ryle reported that he worked under a similar assumption, and accordingly advised colleagues against putting things in writing or emailing if they did not want them to come out afterwards.

Privacy International's Tomaso Falchetta highlighted the hidden nature of some digital acts that can impact on journalists working with confidential sources: "Of significant concern is the fact that digital communication surveillance - sometimes by the use of malware on the target's computer - is usually being conducted in secret so the journalist is not aware of the intrusion and cannot challenge or limit it".

Pedro Vaca Villareal, Executive Director of Colombia's Foundation for Freedom of the Press (FLIP), told this study that investigative reporting practices have already changed in his region in response to the challenges posed by digital surveillance and other factors undermining source protection.

According to Deputy Director of the Tow Centre for Digital Journalism, Susan McGregor, a change of practice in managing digital communications is required in response – at both the personal and professional levels.

> *It means that we have to be thoughtful about our devices and our communications in the way that most of us aren't accustomed to doing yet… Some of the habits we've developed… taking our phone everywhere, always having Wi-Fi on, emailing everything, we're just going to have to think differently about those things when it comes to work with sources. Chances are we'll also think differently about them in our personal lives, rather than trying to juggle two frameworks of communication.*

Sweden's Fredrik Laurin stated: "Anytime there is any chance of the government being interested in what we do, during our research or after publication, I go to great lengths to protect my information. That means applying the strongest encryption I can find, the best methods, throwaway phones, you name it we try to do it." (op cit 2015).

US media lawyer Charles Tobin said that there was a growing involvement of legal counsel in the story production process due to source protection issues:

> *…It's just becoming more and more acute because you have seen more journalists' subpoenaed over the last 10 years than you did over the prior 50 years, and so it's becoming more of the subject of conversation when journalists call for advice. …You look at issues not only of defamation and the lawfulness of the news gathering, but you also have to have a conversation about protecting the sources and how rigorous that needs to be done depending on the journalist's relationship and promises to the source.*

ii. Going back to analogue methods

Bolivia's Ricardo Aguilar from *La Razon* believes that mass surveillance has significantly weakened source protection laws. "The response from journalism should be to make mass surveillance useless, taking excessive precautions when working with secret sources on

issues that affect large economic interest, or persons of economic and political power". (Aguilar 2014)

Alan Rusbridger has questioned if investigative journalism based on confidential sources is possible in the digital age, unless journalists go back to what he calls 'basics': "I know investigative journalism happened before the invention of the phone, so I think maybe literally we're going back to that age, when the only safe thing is face-to-face contact, brown envelopes, meetings in parks or whatever," he said.

Catalina Botero, former Special Rapporteur on Freedom of Expression with the Organisation of American States, advised going back to what she called 'the classics' of journalism practice. "Go to the corner, to a coffee shop, and talk to them. This is like a very huge contradiction because you have these great tools, wonderful tools to do journalism all around the world without moving from your house. But at the same time, you need to ensure that no one else is hearing".

That's the practice being adopted by the lead investigative reporter at Argentina's *La Nacion*, according to the paper's Editor-in-Chief Carlos Guyot: "[He] is now having more conversations face to face than ever before because the vast majority of his sources refuse to talk to him on the phone. Or, at least, he has to agree on new ways to communicate with them - actually, the old fashioned way: using public booths".

UK QC Gavin Millar, who represents several freelance journalists, said that some have a contract phone which they throw into the Thames River at the end of each week. They meet sources in pubs, write notes, and hide the notebooks in distant places in case their houses are searched by police.

Bolivia's Aguilar avoids using digital communication in order to protect his sources.

He said extreme distrust is the only defence against the possibility of confidential sources being exposed through the clandestine interception of email and social networks.

Algerian newspaper editor Zine Cherfaoui said journalists in the Middle East and North Africa, in particular, have become very cautious with electronic communications. "We prefer to meet the person directly and avoid digital platforms. Because of mass surveillance and new anti-terrorism laws we like to avoid social networks".

From the Philippines, Danguilang-Vitug said that caution is routinely exercised. "We continue to be very careful when meeting sources…We take precautions, make sure that our mobile phones are not bugged, use secure phones. We opt for personal meetings rather than e-mails for security purposes. If we have to use e-mails, some sources create separate e-mail accounts when answering our questions. But largely, face-to-face meetings are best".

Simple approaches like stretching the timeline between contact with a source and publication of their leaks have also been used to protect the confidentiality of connections and minimise the chance a confidential source will be identified. ICIJ's GerardRyle said: "The more layers you can put between you and the source sometimes is better, and a lot of that is time. If someone gives you some really hot information the temptation is to publish that right away, but that's also when your source is potentially at most risk." (Ryle 2015).

An editor who responded anonymously to a survey conducted in conjunction with this research highlighted the risks that long-term data retention could lead to identification of a source who was initially not an object of suspicion. Another news organisation's legal

advisor told this study's researchers that it is important to split encryption passwords between two journalists as an added precaution against data interception in the case of the detention of one party.

iii. Taking responsibility for digital security

Swedish public radio's Fredrik Laurin said that journalists are under-prepared when it comes to protecting sources in the 'digital hemisphere'. "Very few journalists use encryption and very few journalists even know how to use it - it's not in their toolbox and that is a major problem," he said. Laurin's hardcore dedication to digital security in the interests of protecting his sources extends to banning certain corporations' products among his reporting team. "We're using open-source material that we can change, where we are in control. Because at the end of the day, source protection is our mandate, our job, also under the law, and therefore we cannot use service providers who do not give us the ability to control the information."

Atanas Tchobanov, the Editor-in-Chief of Bulgaria's investigative journalism website Bivol and its extension, *Balkanleaks*, said that his means of communicating with confidential sources have been evolving alongside his investigative journalism practices since *Bivol* launched in 2010. He assesses who is likely to be eavesdropping and what their technical capability is, and if it is not advanced, then he will use Skype or WhatsApp without feeling the need for further encryption.

In Brazil, there is less concern about mass surveillance but nervousness about targeted monitoring of email and phone lines according to Executive Director of Journalism at Grupo RBS, Marcelo Rech. He said journalists in his organization are increasingly turning to chat apps to protect their sources. "People sometimes use WhatsApp, which is more tough to track…usually the sources prefer to talk by WhatsApp, or in person…" However, confidence in WhatsApp (an encrypted message service which is owned by Facebook) is misplaced, according to journalism safety expert Javier Garza, who advises the World Editors' Forum.

According to ICIJ's Ryle, another practical consideration is that digital security measures designed to protect sources can be unwieldy and time-consuming, and these factors remain a deterrent to many investigative journalists. The need for simple, cheap technological interventions to protect communications with confidential sources from surveillance was also underlined by an anonymous editor who responded to a survey connected to this Study.

The Committee to Protect Journalists (CPJ's) Courtney Radsch pointed out that, conducting meetings or interviews with sources face-to-face is not always possible, nor practicable – particularly on international stories (see also Section 10 below on Gender Dimensions Arising). Fredrik Laurin also reflected on this point in regard to an investigation where "we needed to investigate the situation on the ground in six different countries and it was impossible for us for safety reasons and also practical reasons. We needed to do our investigations digitally, over the phone, over Skype, over Facebook, email. That was a major challenge to employ all the necessary forms of encryption and secure communication".

But ICIJ's Gerard Ryle argued that too many journalists are growing unnecessarily paranoid. "…(T)here are some reporters I know who are completely paranoid about their computers - they're fantastic at encryption, everything is offline. But so what? Most of what they're working on isn't relevant." He said he did not believe that any method of source protection was 100% fool proof.

iv. Avoid flagging source protection efforts

Taking 'radical' measures to secure communications, including using encryption, can actually risk attracting unnecessary attention, Ryle indicated. "You are sometimes better off hiding in plain view". Even providing training in encryption to journalists can attract suspicion, according to Internet Sans Frontiers (ISF) journalist and lawyer Julie Owono.

The flipside, however, is the risk to the safety of journalists if digital technology is avoided, as recognised by Alan Rusbridger. He said: "You want them to have these devices [smartphones] because you want your reporters to be constantly in touch and you want them to file and take pictures, but these devices are also tracking devices." There was a dilemma between the risk of yielding digital information about sources, and having a device to help ensure personal safety, especially in conflict zones, he argued.

f. Training and editorial leadership

There is evidence that some news organisations have been slow to respond to the threat of source protection erosion in the digital age, with concerns expressed by several interviewees and survey respondents about the level of understanding among newsroom managers. Other research also indicates problems with the prioritisation of digital security and training by news organisations (C.f. Posetti 2014c, Holcomb, Mitchell & Page 2015).

However, *La Nacion*'s Guyot told this study: "If we want journalism to survive and flourish in the 21st century, there is no other option than to give our reporters and sources the tools necessary to do their jobs". Internet Sans Frontiers' Julie Owono told the researchers that there has been a significant uptake of digital security training among journalists in Africa and the Arab States since the Tunisian uprising, as reporters have learnt that a single password is not sufficient to provide digital protection.

However, ARIJ's Rana Sabbagh said that even the best training cannot keep up with global intelligence services: "…(W)e train our journalists in encryption and how to protect their data, and tell them to always assume that everything you're doing online, on your computers, is accessible, because even if you give them the best software and training, the intelligence agencies are always a step ahead. They are using the latest technologies to decrypt the content ".

Another point that several interviewees made is that seemingly innocuous local stories can be triggers for anonymous sources to make contact, meaning that a story that starts small can escalate into a major journalistic investigation, potentially causing confidential communications to be exposed through hostile data mining. Also, specialised coverage areas like health, politics, sport and financial reporting are increasingly vulnerable to source exposure due to leak investigations, according to investigative journalists and editors interviewed for this study.

g. Training the sources

"We're significantly increasing the training within the organisation to get this [digital security for source protection] on the radar of reporters to try to help them get around it," Rusbridger said. "But it's one thing to teach reporters, it's another thing to try and educate the public and the sources". He was acknowledging an emerging trend in source protection:

journalists and news publishers taking on a new responsibility - educating their sources in their own protection.

A multi-layered digital security approach, in combination with training and equipping sources to contact reporters securely, is the future of source protection, according to Fredrik Laurin. "You need to be aware of what tools are available and you need to do that yourself and to inform your sources on how to employ these methods". ICIJ's Ryle acknowledged the problem with digital safety practice among sources: "Most people who are outed as sources make the mistakes before they come to the journalist. And they use their own phone, their own computer, they even use an email address that can be traced back to them," he told the author.

Interviewees identified a role for NGOs and professional organisations in the training of sources to communicate more securely in the digital environment, and to support journalists to do the same. For example, the Swedish Union of Journalists recently published a book designed to educate journalists in online source protection called *Digitalt Källskydd*.

That level of source education is already happening at *The Guardian*, albeit in a minor way. A secure electronic dropbox has been launched but Rusbridger said that he doubted that many reporters had successfully gone out and installed PGP[22] on a source's machine and taught them how to use it. *The Washington Post* and a number of other major news publishers have also introduced secure dropboxes in recent years.

There is also a need for sources to take independent steps to ensure their own digital security. "Sources have to share the responsibility with us, they have to believe in the cause they're trying to promote, and it should be a shared responsibility. Both a source, or a whistleblower, and a journalist are aiming for the same thing; expose the wrongdoings and corruption as well as promote good governance," ARIJ's Rana Sabbagh stated.

h. Collaborative strategies

A growing number of regional and international investigative journalism consortia (Alves 2014) has corresponded with an emerging trend of collective and centralised source protection. In its global investigations that involve myriad international publishing partners, ICIJ essentially becomes the source: "We don't take responsibility for the publication of our projects in each country, each organisation has to do that, but in terms of giving them the information, we become the source. In other words, we give them the documents. ICIJ is the source of the material," Director Gerard Ryle said.

Jurisdiction 'shopping' also becomes a strategy for some journalistic actors, who seek to base their digital content in countries with a stronger degree of privacy protections than those where the intended audience is based. This was the motivation for *The Guardian*'s decision to move the Snowden investigation offshore to the US. It is also the reason Bulgaria's investigative journalism website Bivol is based in France, and a new international Francophone collaboration (see discussion of SourceSure below) is anchored in Belgium.

Gavin Millar QC pointed to another important area of collaboration in source protection – between journalists, freedom of expression activists and people he describes as 'good hackers'. "We've done a lot of work with the good hackers in Berlin and in London…we have

22 Developed by Phil Zimmerman in 1991, PGP stands for Pretty Good Protection. It provides cryptographic privacy protection through an encryption and decryption program http://www.pgpi.org/doc/pgpintro/

a stack of wiped laptops in the offices [of the Centre for Investigative Journalism which he chairs], which we sell to investigative journalists at cost price because we're a charity, having got some of the top hackers in the world to devise defence programs for them and to upload those programs to defend…against back door access to their digital material."

Meanwhile, interviewees explained how international news organisations have begun collaborating on platforms designed to securely receive digital information from confidential sources. AfriLeaks, for example, is a Pan-African project that uses a highly secure mailbox designed to receive leaked documents, which connects investigative media houses to whistleblowers. It is operated by the African Network of Centres for Investigative Reporting (Cummings 2015). Mexicoleaks also launched in 2015 (Attanasio 2015).

Sourcesure and Balkanleaks are similar Francophone and Bulgarian websites that allow whistleblowers to upload secret documents anonymously. Sourcesure, which is based in Belgium to take advantage of strong source protection laws there, was jointly established in February 2015 by France's *Le Monde*, Belgian publications *La Libre Belgique* and *Le Soir de Bruxelle* and RTBF (Radio Télévision Belge Francophone). Yves Eudes, Sourcesûre's cofounder and a journalist at *Le Monde*, believes that the cross-border, multi-platform collaboration between leading Francophone news organisations is a source of protection for journalists and sources. "Unity is strength. This initiative could not have been launched by *Le Monde* or RTBF alone. Sourcesûre is underpinned by a whole spectrum of collaborators, from liberal to conservative media outlets, united by common journalistic values," he said. Sources using the system are encouraged to download TOR software at their end before connecting with the system (Eudes 2015).

i. Further issues

For this thematic study, the interviewees were not specifically asked about how the practical precautionary measures discussed here could be complemented with other steps. A holistic approach would include advocacy to secure legal confidentiality to cover cases where technical secrecy or analogue methods proved insufficient. An example would be advocacy to secure legal limits on the use of intercepted digital information about confidential journalistic sources, in regard to admissible evidence in court. Further research could be done in this area as to how experts regard the complimentary range of measures to protect confidentiality.

Thematic Study 2:

How a State with one of the world's oldest and constitutional legal source protection frameworks is responding and adapting to emerging digital threats[23]

Despite the strong legal frameworks that exist, Swedish journalists operate in an increasingly difficult environment in relation to the protection of sources in the digital age. Complications presented include the rapid development of technology and the time lag involved in Swedish legislation adapting in tandem. They also involve the impacts of national security-based restrictions, mass surveillance impacts, and the education and training barriers faced by both journalists and their sources. Collectively, these factors pose a significant challenge

23 Angelique Lu contributed to this case study

in a State that criminalises confidential source exposure and places the onus of responsibility for the preservation of confidentiality firmly at the door of journalists.

This thematic study is based on in-depth online research and long-form interviews with five key actors with expertise in the practical and theoretical issues surrounding Swedish legal source protection frameworks in an era of digital transformation. They include investigative journalists, the national journalists' union, lawyers, academics, and a legal policy specialist responsible for media freedom issues from Sweden's Department of Justice.

1. Strength of traditional Swedish source protection laws

The legal framework in place in Sweden for the protection of sources is based on constitutional provisions. The Swedish press enjoys protections in two out of the four pieces of legislation that comprise its constitution - the *Freedom of the Press Act* as well as the *Fundamental Law on Freedom of Expression* (Banisar 2007). In its earliest form – in 1766 - the Freedom of the Press Act included protection for anonymous authors (Banisar 2007:21; University College London, 2011). This is the foundation of Swedish source protection laws. *The Fundamental Law on Freedom of Expression* (1991) extends these rights to radio, television and 'other technologies', encompassing blogs and websites (Banisar 2007:72 footnote 203; Berglund-Siegbahn 2015.)

In Sweden, a source who divulges information to a journalist on condition of anonymity is protected under the Constitution (*Freedom of the Press Act*, Chapter 3; *Fundamental Law on Freedom of Expression* Chapter 2). In fact, it is a criminal offence for a journalist to breach this confidentiality agreement, regardless of whether the identity of a source is revealed 'through negligence or by deliberate intent.' (*The Fundamental Law on Freedom of Expression*, Chapter 2, Article 5; Nygren 2015). A journalist who reveals the identity of a source may be subject to a prison sentence of up to one year, or ordered to pay fines (*The Fundamental Law on Freedom of Expression*, Chapter 2, Article 5). The identity of sources is protected from disclosure except in limited circumstances, such as a breach of national security and high treason (*The Fundamental Law on Freedom of Expression*, Chapter 5, Article 3; *The Freedom of the Press Act*, Chapter 7; Article 3). Such exceptions must also be vetted by a Swedish court (Trehörning 2015) and Swedish courts are constitutionally bound to place weight on the protection of press freedom in their deliberations (*The Freedom of the Press Act*, Chapter 1 Article 4; *The Fundamental Law on Freedom of Expression*, Chapter 1, Article 5; Berglund-Siegbahn, 2015).

There was overwhelming consensus amongst the Swedish experts interviewed regarding the soundness of the legal framework that currently operates in Sweden (Berglund-Siegbahn, 2015; Laurin 2014, 2015; Nygren 2015; Trehörning 2015). According to media lawyer and Press Ombudsman Pär Trehörning: "The legal (framework) is very strong because it's a part of our constitution. The person who gets information from a source…can't reveal that. The only exception is in court, and it's extremely seldom".

Anita Vahlberg, senior advisor to the President of the Swedish Union of Journalists, stressed the significance of the constitutional requirements placed on journalists: "The constitution provides for protection of sources which is not a right for journalism, it's an obligation to protect your sources" (Vahlberg 2015). According to Vahlberg, this obligation underpins Swedish journalism practice: "Swedish journalists take the question of protection of sources very seriously," she said.

There is some debate over the criminalisation of source disclosure by journalists, and whether it places an unfair burden on journalists to protect their sources in the digital era. Global Freedom of Expression organisation *ARTICLE 19*, raised issues in a paper discussing Tajikistan's 2013 media law proposing an analogous legal obligation on journalists not to reveal the identity of their sources:

> *Article 26 [of the Tajikistan media law] reverses traditional presumption not to disclose information. Although the matter has never been dealt with by an international court, there are potentially serious problems with imposing source confidentiality as an obligation on the media and it would be preferable for Tajikistan to follow the dominant practise in this area.* (ARTICLE 19 2014, p.18).

ARTICLE 19 argues in the case of Tajikistan that source protection should be a legal right, not a legal obligation. The Knight Center for Journalism in the Americas' Silvia Higuera stated, in an interview with this Study's researchers, that a journalist should not be held accountable if their sources were exposed as a result of surveillance or other issues connected to their digital practice: "I want also to be clear…our obligation to protect our information doesn't mean that when a journalist's communications are intercepted, it's her or his fault. The journalist is still the victim, and abusers should be prosecuted" (Higuera 2015).

Nevertheless, those who stand by the criminalisation of the revelation of a confidential source's identity without their permission, believe this onus to be core to the success of the existing legal framework to date. It is seen as not just protecting the journalist, but also ensuring that a source is confident to divulge information on the understanding of anonymity. It is not clear, however, how the Swedish courts might interpret a journalist's responsibility to ensure the digital security of their communications with confidential sources to avoid their unmasking through interception or bulk data analysis, for example. This is an issue that may require testing in terms of the measures considered to be reasonably required of journalists to secure their digital communications to avoid legal liability if their sources are exposed.

2. Applying the Certificate of No Legal Impediment to Publication online

Journalists in Sweden do not require tertiary qualifications to practise journalism, nor are they required to have such qualifications to be eligible for protections under the constitution (Laurin 2015, Berglund-Siegbahn 2015). However, publishing platforms do require registration for the purpose of accessing certain protections. Protections found in the Swedish Constitution apply to the registered medium and not the individual journalist (Laurin 2015; Nygren 2015; Berglund-Siegbahn 2015). Thus, the eligibility for protection is for the platform, not the individual as such, and there are variations here. Thus, traditional forms of news media are automatically covered by Swedish constitutional press protections (Berglund-Siegbahn 2015), however Swedish law prescribes a number of additional requirements that would need to be met in order for websites to qualify for source protection.

According to the editor of the investigative department at Swedish Public Radio, Fredrik Laurin, the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, despite being written in 1949 and 1991 respectively, were arguably drafted in wide enough terms to encompass bloggers:

> *…The law applies not to the journalist as some kind of certified individual, source protection law applies to anyone who is willing to divulge important information for the purpose of having it published. It doesn't define who you divulge this information to.* (Laurin 2015)

However, on the publishing side, a website or publication with a Swedish Editor-in-Chief must be certified if it wishes to be covered by Swedish source protection law. It is common for niche and start-up websites and blogs to have only one contributor, who would also need to be considered the Editor-in-Chief in this context. In this mode, those who are not members of traditional media, such as bloggers, social media actors or people creating a new website, can choose to apply for a 'certificate of no legal impediment to publication' in order to enjoy Swedish constitutional coverage for periodicals including source protection provisions. Individuals or groups wishing to certify their website under this structure gain the same protections as traditional media (for example in regard to a degree of libel protection) as well as responsibilities, which include the legal obligation to protect source confidentiality (Berglund-Siegbahn, 2015, Laurin, 2014, 2015).

The provisions governing the 'certificate of no legal impediment to publication' include the requirement that the website has a uniform appearance across its pages, it cannot be altered by anyone other than editorial staff, and an Editor-in-Chief must be appointed who is liable for any violations of provisions governed by the Constitution (Fundamental Law of Freedom of Expression: chapter 1; article 9). Further, the Editor-in-Chief must satisfy a number of 'required qualifications' (The Freedom of the Press Act Chapter 5) which stipulate, inter alia, that the would-be-editor must live in Sweden, be aged above 18 years, and must not be an undischarged bankrupt or under guardianship (The Freedom of the Press Act, Chapter 5, Article 2). In an analysis conducted by the Association for Progressive Communications (APC), the additional obligations and protections offered by registering a website under the Swedish constitution was analogous to that of a boxing ring:

> *Boxers enter the ring knowing that in the ring certain rules apply, protecting them from illegal actions; but they are at the same time subject to certain physical risks that are allowed by the same rules that protect them in the first place. The risk of taking on the liability of being a responsible editor is something the editor would have to accept to be able to enjoy the benefits of source protection, inquiry protection and prohibition of censoring.* (Almström, H, 2011).

The experts interviewed for this thematic study were asked if the application for certification process in Sweden is actually a form of licensing. They highlighted that it is a voluntary process and does not prohibit anyone from publishing without a certificate. It is not required for a blogger to have a 'certificate of no legal impediment', and there is also no legal basis to withdraw a certificate (where issued) for reasons of content. The interviewees were reluctant to even call the certification process 'registration' due to their rejection of registration procedures used in other contexts to deny or cancel the status of a person or platform seeking to publish journalism. (Berglund-Siegbahn, 2015; Laurin 2014, 2015; Nygren 2015; Trehörning 2015).

Non-traditional media publications without a 'certificate of no legal impediment', are instead covered by a third part of the constitution titled the Instrument of Government (Chapter 2, Article 1), and its provisions for fundamental rights and freedoms, as well as by provisions under the European Convention for Human Rights (Berglund-Siegbahn 2015; Axberger 2015). In an interview for this Study, Hans-Gunnar Axberger, Professor of Constitutional Law at the University of Uppsala, maintained that the strong protections for journalists

contained within the Swedish legal framework have been upheld in the context of new technological developments. But he pointed out related issues where expectations have changed and clarity is reduced. "For a source who provides information to a blogger who has not obtained a 'certificate of no legal impediment', there is potentially an uncertainty as to the strength of what the expectation of anonymity can be which they may not even be aware of themselves", he said. Furthermore, he pointed out that while protections for authors of texts and their sources remain strong, the subjects of online content produced by non-traditional media are in a much weaker position when it comes to accessing legal recourse than is the case with traditional media (Axberger 2015).

3. Swedish source protection may not extend to digitally stored content

Swedish authorities are generally prohibited from seizing journalistic materials that may reveal the identity of a source (Laurin 2014; Trehörning 2015, *The Fundamental Law on Freedom of Expression*, Chapter 3, Article 5). There are exceptions, however, as Laurin points out. "For example, in the Swedish Criminal Act, there are possibilities for the police to do a house search and if they suspect me of a crime, they can come to my house and they can break in and they can grab equipment, paper work, computers …". Nevertheless, "... source protection is paramount and therefore the police cannot go through documents in the newsrooms that contain source protected information. That has to be dealt with (via) a special order where the court appoints special measures to protect the source," he said.

However, while hard copy material (e.g. notepads and paper files) kept by journalists that may reveal the identity of sources are constitutionally protected from police searches under the conditions described above (*The Fundamental Law on Freedom of Expression* Chapter 2, Article 4; Berglund-Siegbahn 2015), the same protections do not automatically extend to digitally stored materials – such as recording devices, discs, smartphones, portable hard drives, and computers (Berglund-Siegbahn, 2015; Laurin 2014; 2015).

This source protection gap was illustrated in a case involving journalist Trond Sefastsson, who was investigated by Swedish authorities in 2007 in relation to allegations of bribery and tax evasion (Andersson et al 2012). A search warrant was executed in the course of the investigation and digital equipment, including a computer containing information that could reveal sources' identities, was seized. The seizure was met with opposition by members of the National Press Club as well as TV4, the television channel which employed Sefastsson, (Hamrud, 2007). Fredrik Laurin said this is an area where the Swedish law needs to be updated.

Members of the Swedish media also said the seizure of Sefastsson's data could impact on citizens' confidence in a journalist's ability to protect their sources (Hamrud, 2007). Some expressed concern over what they saw as the disproportionate nature of the seizure compared with the allegations (Hellberg 2007). The Deputy Chief Prosecutor in the Sefastsson case, Björn Blomqvist has resisted these suggestions and criticisms. His argument hinged on the potential for journalists facing criminal allegations to delete incriminating evidence during an investigation (Hamrud, 2007). In October 2008, a Swedish court ruled that police authorities had the right to retain Sefastsson's computer because of the serious nature of the allegations levelled against him, despite the fact the computer contained material relating to his work as an investigative journalist over the course of a decade.

There have been a series of cases since the Sefastsson case in 2007 that have implications for the protection of sources in Sweden. In March 2011, in an operation designed to combat child sex tourism, Swedish customs and police officers raided the premises of 28 people. Among them was Swedish journalist Bertil Lintner, whose computer and phone were searched in his absence (Folkbladet 2015). In another case, Sveriges Radio correspondent Nils Horner was killed in Afghanistan in March 2014. After his death, many of his belongings were confiscated by the International Public Prosecution Office, including computers and notebooks. The District Court decided that everything would be returned to his estate except for his computers, sim cards and mobile phone. In October 2014, however, all equipment was returned to Sveriges Radio (Folkbladet 2015). Also in October 2014, a Dagens Nyheter (DN) photographer's camera memory card was seized by the Swedish military because it contained pictures of a military prohibited area. The military seized the memory card, which contained 47 images. Under the Sweden constitutional laws *The Fundamental Law on Freedom of Expression's* and the *Freedom of the Press Act's* provisions for 'anskaffarfrihet' and prohibition against censorship, everyone has the right, subject to freedom of expression provisions, to procure data in any subject for the purpose of publication and to publish anything without prior scrutiny of authorities (Högsta Domstolen 2015). The DN photographer claimed that the photos taken were protected under the "anskaffarfriheten" provision. In June 2015, the Supreme Court declared that the constitutional provisions outweighed the law on protection of prohibited areas.

In another case, in March 2015, Swedish Police in the course of a murder investigation seized the phone and laptop of *Folkbladet* journalist Elin Falk who had been the victim. *Folkbladet* Editor-in-Chief Anna Lith objected, stating that the seizure of materials was incompatible with Swedish constitutional protection of sources (Hellberg 2015). The Lycksele District court upheld the seizure of Falk's phone and computer but ordered the return of her notepad. The Court also found that the electronic items could be searched and that the proceedings would be conducted behind closed doors. The decision was immediately appealed by Lith and *Folkbladet*. The Court of Appeal's decision rested on the question of whether the prohibition of the confiscation of written documents could extend to electronic information. Under Swedish law, written documents cannot be confiscated if the documents can be presumed to contain information given by a source under the condition of anonymity under Swedish constitutional law. In its decision, the court stated that the decision required a balance between two competing considerations, a criminal investigation and the need to protect the anonymity of sources as stated under the Swedish constitution.

However, while the Swedish Court of Appeal acknowledged that electronic information was equally important to written information, it found that it would not be permissible to ban the confiscation of electronic storage devices whenever there was a risk that the identity of a source could be revealed. One of the factors that influenced the court's decision in this regard was the presumption that electronic content could be searched specifically without revealing other information (e.g. via keyword searches), distinguishing it from written documents. However, the Swedish Court of Appeal took into account the broad nature of the search parameters by the Swedish Police, stating that because the investigation did not know what it was specifically searching for, the search would constitute the violation of an individual's right to submit information to the media anonymously. The prosecutor proposed that a representative from *Folkbladet* be invited to attend the examination of the computer and mobile phone. However, the Swedish Court stated that there was still a risk of exposing a source due to the broad nature of the general search by prosecutors. The Court of Appeal ultimately decided that for these reasons the prosecutor's submissions to seize

the computer and mobile phone could not be considered to outweigh the constitutional interest to protect the identity of sources.

In 2011, a report was published by the Statens Offentliga Utredningar (Swedish Public Inquiry) investigating, among other things, seizures conducted by public authorities (Statens Offentliga Utredningar 2011). Legal advisor at the Ministry of Justice Division for Constitutional law Katarina Berglund Siegbhan told this study that the following recommendation was proposed:

> *If a computer or another digital information carrier is seized, and may contain protected information – for example information covered by the rules about protection of sources – the person from which the computer is seized should have the opportunity to be present during the examination of it. If protected material is found, the person who performs the examination immediately must stop [viewing] this material.* (Förundersökning; SOU 2011:45)

The commission's proposal was being considered by the Swedish Government at the time of writing.

A number of other approaches for updating Sweden's source protection frameworks have been suggested. Swedish media law academic Hans-Gunnar Axberger proposed that prosecutors should go before a court ahead of seizing a journalist's computer in the future (Hamrud, 2007). Swedish media lawyer Pär Trehörning proposed to researchers a safeguard through an independent third party who would assess the content to determine whether there is information revealing the identity of a source. However, as Trehörning recognised, this presents a conundrum: how does the independent third party protect such information? Once a party has seen content, including the identity of a confidential source, they cannot 'unsee' it.

Swedish Radio's Laurin said that until this discrepancy in source protection law is addressed, Swedish journalists and their sources will remain vulnerable.

4. Implications of interception, surveillance and data retention

As discussed in the regional overview section of this Study, new anti-terrorism laws were passed in Sweden in 2009, authorising the National Defence Radio Establishment (FRA) to access and store all telecommunications (including domestic communications) that cross the country's borders via cable or wireless. There are no exemptions for journalistic communications. According to a European Parliament study *National programs for mass surveillance of personal data in EU member states and their compatibility with EU law* (Bigo et al 2013), Sweden is becoming an increasingly important partner of the global intelligence network, engaging in operations and programmes for the mass collection of data. According to the EU report, FRA has been undertaking bulk 'upstream' collection of private data – content and metadata – where communications crossed Swedish borders.

These developments may impact on Sweden's historically strong legal source protection frameworks. In the *Folkbladet*/Falk case discussed above, the Swedish Supreme Court found that the seizure of digital journalistic communications data could be supported if the terms of the search were sufficiently narrow to avoid wholesale exposure of sources. However, in the context of mass surveillance, it may no longer be technically possible for journalists to promise protection from exposure to their confidential sources when they involve digital communications that cross Sweden's borders.

5. Lack of applicability of Swedish source protection to social media platforms in Sweden

The protections provided by the existing Swedish legal framework and the 'certificate of no legal impediment' to publication do not extend to acts of journalism published on social media platforms such as Facebook and Twitter, whether they are performed by bloggers or professional journalists as curators and editors of their own accounts. The legal experts interviewed agreed that this may present issues for any social media actor who uses these platforms to publish material based on confidential sources in Sweden.

Katarina Berglund-Siegbahn, legal advisor at the Ministry of Justice Division for Constitutional law, recognised that "it might be quite strange of course that you can say it somewhere and have to protect your sources when you write something on your blog, and you don't have the same protection on Facebook".

Journalist Fredrik Laurin maintained that the current legal framework offered in the Swedish constitution provided adequate protection. According to Laurin, any additional provisions protecting content published on social media would be unnecessary. But media academic Dr Gunnar Nygren from Stockholm University told the researchers: "[I]t's important that all kinds of media outlets, no matter what platform have the same sort of source protection. Even if it's a website. All platforms should have equal kinds of laws".

Social media platforms and chat apps present additional problems in relation to source protection in Sweden. Issues regarding transparency by such third party intermediaries, the fact they are generally under foreign jurisdiction, along with potential pressure for data handover within these jurisdictions, are other problems identified by Laurin. As a result, mindful of being bound by the Swedish constitutional obligation that binds him as a professional journalist to protect his sources, Laurin has actively boycotted such platforms.

6. Practical Moves/ The Journalist's Obligation

The legal obligation placed on Swedish journalists to protect their sources is complicated by digital developments. Consistent with trends presented in other regions in this Study, Swedish journalists are faced with difficulty in protecting their sources in a mass surveillance environment. According to Anita Vahlberg, senior advisor to the President of the Swedish Union of Journalists:

> *Our major problem is not legal protection. That's part of the Swedish constitution. The law is solid. The problem is more practical when it comes to protecting sources when email, telephones, everything is monitored by one or many authorities, sensitive information…can be monitored [and] can be hacked by others.*

There have been moves by the Swedish Union of Journalists – so far unsuccessful – to introduce exemptions for journalists - in particular for freelancers - from anti-terrorism legislation, data retention provisions and the monitoring of telephone communications, as these functions may undercut source protection (Vahlberg 2015).

Swedish journalists have also suggested defensive responses dependent upon changes in journalistic practice. According to Fredrik Laurin: "What I see is a change in behaviour from a practical point of view, it's not so much legal but it's much more a question of how we as journalists handle the information in reality". Approaches identified include the employment of encryption techniques, being cognisant of where servers are held, as well as the laws

that regulate the data in the country in question, and actively boycotting externally owned companies and products.

Consistent with the broad findings in the overarching study, some of the experts interviewed for this thematic study encouraged reporters and sources to use analogue methods of engagement with confidential sources, such as meeting in person, using paper, avoiding emails, using so-called 'dumb' phones, and so on in order to avoid surveillance, data retention and digital equipment seizure.

The Swedish Union of Journalists, in collaboration with other Swedish organisations, has published information booklets educating journalists on appropriate practises, while Swedish public broadcasters have implemented technical training for employees. However, this kind of response is also recognised as having limits in terms of decreasing resources in newsrooms, especially with regard to regional, rural and independent media (Vahlberg 2015; Trehörning 2015).

7. Education of Sources

Swedish media experts have also suggested the education of sources as a means of assisting in preserving their confidentiality. Journalists' union lawyer Pär Trehörning stated that first contact between a source and a journalist may be problematic in the protection of sources and thus the only way to improve digital security at that point would be to provide training to sources and the public broadly.

8. Conclusion

Despite reliance on what is a very strong traditional legal framework for source protection, Swedish journalists, like journalistic actors in other countries, are facing difficulty maintaining their commitment to source confidentiality in the digital age. The legal obligation on Swedish journalists to protect their sources may become increasingly complex, placing both journalists and their sources at greater risk. The primary threats come in the form of digital reporting practices, surveillance, data retention, the seizure of digitally stored information, a lack of protection over social media platforms, and digital companies falling under different jurisdictions. Gaps in the country's source protection have emerged as a result.

Thematic Study 3:

Towards an international framework for assessing source protection dispensations

This thematic study maps the development of an 11-point framework for assessing the effectiveness of legal source protection systems in the digital era. It draws on interviews with 31 international experts across all five UNESCO regions. These experts span the areas of law, human rights, academia, professional journalism, and ICT experts. The interviews were conducted in person, via Skype, telephone and email between November 2014 and May 2015. Based on initial study of the issues, and in consultation with UNESCO, the researchers presented a draft eight-point standard for the experts' consideration. It was then developed and expanded into an 11-point assessment tool, based on the experts' input, in the course of this thematic study.

The emergent assessment tool is designed to be applicable to all international settings for measuring the effectiveness of legal source protection frameworks within a State, in the context of established international human rights laws and principles.

Experts interviewed:

1. Professor Rasha Abdulla (Media Studies academic, Egypt)
2. Ricardo Aguilar (Investigative journalist, La Razón, Bolivia)
3. Catalina Botero (former Special Rapporteur, Freedom of Expression, Inter American Court of Human Rights, Latin America)
4. Peter Bartlett (Barrister specialising in media law, Australia)
5. Cliff Buddle (Senior Editor, South China Morning Post, China)
6. Umar Cheema (Centre for Investigative Reporting, Pakistan)
7. Zine Cherfaoui (International Editor, El Watan, Algeria)
8. Marites Dañguilan-Vitug (Investigative journalist, Philippines)
9. Tomaso Falchetta (Privacy International)
10. Javier Garza (Journalist/Journalism safety expert, Mexico)
11. Silvia Higuera (Journalist, Knight Centre for Journalism in the Americas, Latin America)
12. Daoud Kuttab (Journalist/Media freedom activist, Jordan)
13. Fredrik Laurin (Director Investigative Department, Swedish Public Radio)
14. Professor Renaldo Lemos (Director of the Institute for Technology and Society, Brazil)
15. Justine Limpitlaw (Legal expert – electronic communications, South Africa)
16. Henry Maina (ARTICLE 19, Kenya)
17. Susan McGregor (Tow Centre for Digital Journalism, USA)
18. Toby Mendel (Executive Director, Centre for Law and Democracy, Canada)
19. Gavin Millar QC (Lawyer/Chair of the Goldsmith's Centre for Investigative Journalism, UK)
20. Peter Noorlander (Chief Executive Officer, Media Legal Defence Initiative, UK)
21. Leanne O'Donnell (Law Institute of Victoria, Australia)
22. Alan Rusbridger (Editor-in-Chief, *The Guardian*, UK)
23. Rana Sabbagh (Executive Director Arab Reporters for Investigative Journalism, Jordan)
24. Josh Sterns (Journalist/Director, Journalism & Sustainability, Geraldine Dodge Foundation, USA)
25. Charles Tobin (Media lawyer, US)

26. Pär Trehörning (Lawyer/Press Ombudsman, Sweden)
27. Pedro Vaca Villareal (Executive Director, Foundation for Freedom of the Press, FLIP, Colombia)
28. Professor Dirk Voorhoof (Media law academic, Belgium)
29. Professor George Williams (Constitutional Law expert, Australia)
30. Prof Wei Yongzheng (Professor of Media Law, University of China)
31. Jillian York (Executive Director, Electronic Frontier Foundation)

Unless otherwise indicated, all sources were interviewed between November 2014 and May 2015.

Interest in a universal framework

The expert actors interviewed for this case study saw value in a universal framework for effective legal source protection internationally.

Executive Director of Canada's Centre for Law and Democracy Toby Mendel contextualised the role of such an international framework. "Although there have been a few international cases on this subject – most commonly at the European Court of Human Rights – these only address the specific issues raised on the facts of the cases and leave many issues unclear. The development of a model law on this issue could be useful as well. I would also like to see countries adopting best practice legislation in this area". The head of the Media Legal Defence Initiative (MLDI) Peter Noorlander pointed to a Council of Europe policy statement on legal source protection as a useful starting point. However, Executive Director of Arab Reporters for Investigative Journalism (ARIJ), Rana Sabbagh, cautioned about political will to implement such a framework by a number of States.

1. Draft Assessment Framework

The draft that emerged from the initial research process was presented to the expert interviewees as an eight-point framework for review. Their comments and concerns are discussed under each proposed point below.

In the draft, it was suggested that a source protection framework might:

1. Recognise the ethical principle and value to society of source protection

"I support this because it is a basic premise in journalism. It will help the public understand the importance of unnamed sources," Philippines investigative journalist Marites Danguilan Vitug said, reflecting the views of most of the interviewees.

However, Toby Mendel disagreed: "I don't think it is appropriate for such a law to recognise an ethical principle. Rather, it should recognise the human rights foundation for source protection, which, under international law, is based on the right of the public to receive information, and not the right of journalists or others to disseminate it, because then it would need to attach to anyone who disseminated information, i.e. everyone".

Belgian media law Professor Dirk Voorhoof made a similar point regarding the international human rights law underpinning source protection. Columbian press freedom activist Pedro

Vaca Villareal also recommended the alteration or withdrawal of this principle, because "… legislating journalistic ethics can be tricky". However, others pointed to the fact that law is often built on principles of ethics.

2. Recognise that protection extends to all acts of journalism, defined in inclusive terms

Egyptian academic Dr Rasha Abdullah said that protection should cover any medium, and encompass blogs and tweets.

USA media lawyer Charles Tobin commented on the issue of whether there should be a 'regular practice' test to identify what counted as journalistic acts (as applied in several jurisdictions). He opposed such a criterion: "a first time freelance journalist who places an article in the public interest in a notable forum is entitled to be treated as a journalist for most purposes, including source protection".

Toby Mendel acknowledged a need to define 'acts of journalism' and pointed to the possibility of exceptions. "I do not believe that source protection should attach to journalists but, rather, to the social activity of disseminating information of public interest to the public - which might well exclude certain journalistic functions. There would also need to be definitions of 'information'[such as] what sorts of communications are covered as well as of sources".

The idea of applying a 'public interest test' to measure the validity of an act of journalism for the purpose of source protection coverage is complex. While the investigative journalists interviewed expressed belief in the value of a public interest test, they had difficulty defining it. The legal experts' views differed. Charles Tobin favoured the inclusion of a public interest test to measure the validity of an act of journalism for source protection coverage. "It has to turn on the specific public interest that was served, the specific purposes that the journalist had in mind, the means that they employed and any other factor that is relevant". For him, public interest had to "be something that serves a larger public discussion on an issue that has mass effect or interest".

However, UK QC Gavin Millar argued that a public interest test presents potential danger, particularly where the public interest element is not clear-cut, and where judges could use a restrictive understanding of 'public interest journalism' to require source disclosure while trying to navigate the middle ground between confidential sources about celebrity tattle and revealing government corruption. Such territory, Millar argued, needs to be resolved on a case-by-case basis.

Former *Guardian* Editor-in-Chief, Alan Rusbridger, proposed that some acts of journalism should not enjoy the privilege of source protection. "If all they're doing is collecting the information on the sex lives of footballers, why should there be any protection for that?" he asked. US journalist and press freedom advocate Josh Stearns thought the public interest motivation needed to be untainted. "I do think something around the idea that they are not publishing this to extract vengeance or blackmail, and it is indeed in the public interest, is important".

ARTICLE 19's Director in East Africa, Henry Maina, made the point that protecting the 'public interest' also serves another function: "We need to ask for due processes that continuously balance and protect our rights and the public interest, as opposed to just protecting journalists as an entity…".

Public interest is also used to justify arguments against granting journalists source confidentiality. At a meeting on source protection in the UK, former senior civil servant Sir David Omand reportedly said that the public needs to know that those who work in public service can be trusted with confidential information. "That, too, is a public interest and a mighty strong one in my point of view to weigh alongside the protection of journalists' sources". A different perspective at the same meeting came from *The Guardian*'s Rusbridger, who was reported as saying that when protection of sources "is done in the public interest, society as a whole benefits from these conversations and these relationships". He further stated: "We have to keep reminding ourselves and other people why as journalists we understand that much if not most of the information that that we receive of value comes from people who are not authorised to talk to us. Or who can talk more honestly if they can talk secretly" (Ponsford 2015b).

The issue of acts of journalism leads into the question of how protection may be relevant to a range of actors performing these acts. Professor of Law at Rio De Janeiro State University Ronaldo Lemos stated: "In the capacity of a member of the Social Communications Council in Brazil, headquartered in the Brazilian Congress, I have supported that those laws should apply to all professional information gathering agents. This is still a loose term, but it denotes that not only 'journalists' deserve source protection laws".

Colombian journalist Silvia Higuera said that source protection laws should apply to "acts of communication or information" (Higuera 2015). She said she would define such acts as having the purpose of communicating or informing audiences about issues of public interest. "Of course, I'm referring to information that is accurate, fair and has other qualities of what is traditionally known as journalistic information. …people who do that should be protected". Higuera also referred to the definition of journalists provided by the Office of the Special Rapporteur for Freedom of Expression of the Inter American Court of Human Rights in its 2013 report *Violence Against Journalists and Media Workers* which states that journalists are individuals who "observe and describe events, document and analyse events, statements, policies, and any propositions that can affect society, with the purpose of systematizing such information and gathering facts and analyses to inform sectors of society or society as a whole" (Botero 2013 p2). It follows from this definition that media workers and support staff would be included, along with citizen journalists.

FLIP's Pedro Varca Villareal expressed an even broader view: "…protection should be as broad as possible and should refer to any person making a diffusion of information or opinion with public purposes by any virtual environment".

While the boundaries of what is journalism may vary according to perspectives, there is recognition that the practice can be done by individuals who are not fulltime or professional journalists, but who nevertheless may rely on confidential sources in the public interest – as interpreted on a case-by-case basis. Not everyone who does journalism is a journalist, but the argument for source protection nevertheless applies to such cases where the output constitutes information in the public interest.

3. Recognise that source protection does not entail registration or licensing of practitioners of journalism

There was overwhelming support for this principle by the experts.

4. Affirm that confidentiality applies to the use of any collected digital personal data by any actor

There was some confusion and misinterpretation among the experts interviewed in response to this proposed principle. It has since been amended (see final framework recommendations below), but at the time of interviewing, it was explained that this point referred in actuality to third party intermediaries.

The Tow Center's Susan McGregor stated that there needs to be more responsibility and accountability within organisations and companies that routinely collect personal data:

> *…as a company you cannot collect data if you cannot adequately protect it. The truth is most companies can't. You have to be able to demonstrate the ability to adequately protect any consumer data you're going to collect and centralise if you're going to collect it. I think if you put that restriction on it, companies will collect a lot less data.*

Algerian newspaper editor Zine Cherfaoui went further, requesting measures to prevent email providers and social media companies handing over journalists' data to the authorities. "We would like those responsible, or in charge of social networks, to guarantee the inviolability of email exchanges, basically that no one hands over emails, especially when concerning journalists," he said.

That is a point supported by Australian digital media law specialist Leanne O'Donnell who was concerned about a data retention laws in her country, which she feared could effectively undermine source protection laws. O'Donnell advocated for a data retention exemption for journalistic communications to ensure that law enforcement agencies could not request data pertaining to journalists' interactions with their sources, consistent with international source protection standards:

> *That's what the Court of Justice of the EU recommended in their decision in April (2014) where they invalidated the EU data retention directive. Because one of the issues with the EU approach was there was no recognition that with certain information in our society there's an expectation that the information is confidential, information such as communications with journalists and communications with lawyers, for example.*

However, Toby Mendel from the Centre for Law and Democracy disagreed with the inclusion of principle 4 in the framework. He said that source confidentiality was a different idea to data protection, which had its own rules. From another perspective, a principle applying to third parties could be seen as shifting the onus of responsibility for source protection from the journalist or the State to the third party intermediary. In Sweden, under existing law, it is the journalist who would potentially face charges if the source was revealed by the third party. Investigative journalist Fredrik Laurin said "…(S)ource protection is something that I am bound to uphold personally. It's me, Fredrik who goes to prison if you are my source and I lose my notebook at the bar and your name comes out because of that. That's my fault and I go to prison. That's why I don't use Gmail for example. Or Facebook". He added: "I need to survey – which I do, very thoroughly – who my suppliers are. I know exactly where my server is, I know exactly what the contract says, the hard discs in that server are named in my name. With my phone number. There's a tag on the material that says this material is protected according to the Swedish constitution".

Generally, a journalist should not be blamed for negligence of a third party, but it is also clear that securing confidentiality at the level of intermediaries does not obviate the roles of both the journalist and the source.

5. Define exceptions to all the above very narrowly in terms of purposes allowing limitation of the principle

Professor Rasha Abdulla argued that the provision for exceptions to source protection was problematic because such exceptions are too often abused, especially in the name of national security. However, ARTICLE 19's Henry Maina said there was a need for exceptions to source protection, such as where a journalist knew the identities of people involved in terror attacks. "…We need to clearly understand the right to maintain the confidentiality of sources is not an absolute one," he said.

Toby Mendel said that no State would adopt a source protection rule without having exceptions, and the key issue was how to define the exceptions.

Silvia Higuera from the Knight Centre for Journalism in the Americas highlighted the importance of this principle: "We must understand that there are some exceptions to all rules, particularly in this time of terrorism threats, but especially because freedom of expression is not an absolute right".

FLIP's Pedro Vaca Villareal said it would be "…important to have the proposal come from the community of press freedom which would be timely and would specify those exceptions. Leaving it to the discretion of governments may mean that exceptions are broad and vague".Alan Rusbridger articulated the need to tightly limit exceptions.

6. Define exceptions as needing to conform to the necessity provision, in other words, when there is no alternative

Gavin Millar QC suggested that an appendix of definitions and exemplars, to assist with legal argument in cases where the 'necessity provision' is tested, should ultimately accompany a legal source protection framework. Specifically, he thought the 'Goodwin Principle' should be referenced. UK Journalist Bill Goodwin won a landmark case in the European Court of Human Rights in 1996 in which the judge ruled that a journalist could not be compelled to reveal a confidential source, unless there was an "over-riding requirement in the public interest" (ECtHR 1996). Millar called for practical examples of categories of cases where an exception to protection might just be acceptable, in order to rule out the ones where it would not be acceptable.

Toby Mendel suggested that the principle needed to go further to articulate additional protections. He supported Millar's view that there need to be explicit examples of exceptions provided in order to avoid abuse by authorities. "Of course, any restriction on freedom of expression must meet the necessity standard but the issue is: what does this imply in the context of source confidentiality? I think the idea of a lack of an alternative means of accessing the information is an important concept here, but it only takes us so far, as law enforcement authorities often cannot obtain the information elsewhere. We need further protections".

Tomaso Falchetto from Privacy International recalled that the Council of Europe's Council of Ministers' 1996 recommendations on protection of sources in national security situations had noted: "Having regard to the importance of the confidentiality of sources used by journalists in situations of conflict and tension, member states shall ensure that this confidentiality is respected". In addition, Falchetto pointed to the 2005 call by the Council of Ministers "on public authorities in member states: [...] to respect, in accordance with Article 10 of the European Convention on Human Rights and with Recommendation No. R (2000) 7, the

right of journalists not to disclose their sources of information; the fight against terrorism does not allow the authorities to circumvent this right by going beyond what is permitted by these texts".

7. Define an independent judicial process, with appeal potential, for authorised exceptions

Charles Tobin proposed that there should be rules in place in any agency that can issue a subpoena to reveal the identity of a source. These rules should involve deep deliberation, approval at the highest level and pre-engagement before the issuance of any subpoena or search warrant for a journalists' confidential source.

Alan Rusbridger also called for "a high and independent hurdle" so that it was not a case of one policeman authorising another policeman to access journalists' data.

While journalist and founder of the Arabic Media Internet Network, Daoud Kuttab, welcomed this provision as a "very helpful mechanism", Marites Danguilan Vitug pointed to issues with the independence of the judiciary in some States where the judicial system can be politicised.

Charles Tobin also argued for an adversarial framing of the 'independent judicial process' in the context of a request to access a journalists' confidential data, and for this to involve transparency so that the journalist would be entitled to an advocate, and have access to all arguments and information.

Gavin Millar QC pointed out that some countries have used covert requests for access to journalists' data (including metadata). "You get the judge involved but still the journalist doesn't know about it. And the position of the NUJ (National Union of Journalists), and the International Federation of Journalists, and most journalist organisations in this country, is that that's not enough. The issue is do you put the journalist on notice of the possibility? Then you can't just have covert access to journalistic source material".

As discussed in section 2.c below, the issue of transparency of process is linked to this Principle 7, but raises further issues. However, an independent judicial process with appeal potential and adversarial framing may be institutionalised even in the absence of full transparency.

8. Criminalise arbitrary and unauthorised violations of confidentiality of sources by any third party

Silvia Higuera from the Knight Centre for Journalism in the Americas said this point should be in law and that violations of source confidentiality should be prosecuted. Toby Mendel agreed with this principle, as long as the 'unauthorised violations' were also deemed to be 'wilful' (i.e. that they included the necessary intention which is required to be guilty of a criminal action). Stronger laws governing surveillance and data retention by companies are necessary for the sake of source protection, according to the Tow Center's Susan McGregor.

Marites Danguilan Vitug argued that sanctions needed to be added to this principle, as did Henry Maina who said that sanctions must be clearly defined. Maina also pointed out: "Care needs to be taken with criminalising arbitrary and unauthorised violations, though, to ensure this does not restrict the very freedom of expression it is intended to protect".

Journalism safety expert Javier Garza Ramos indicated that that there is a need for sanctions to be applied to those parties seeking to subject journalists, and by extension their sources, to surveillance: "If you're going to extend legal protection for journalists for sources, then there should also be some legal consequence on surveillance of journalists, or on anybody, not just journalists. It should be at least prosecution and jail time for whoever is doing illegal surveillance, unauthorised surveillance".

However, Professor Ronaldo Lemos, Director of the Institute for Technology and Society in Brazil, expressed scepticism about such mechanisms and Principle 8 (as proposed here):

> *I think the rule would need to define the types of situations to which it applied, so as to cover all situations, including indirect ones, in which actions led to source exposure. The law would also need to define very carefully what exactly those covered by source protection are due (or what rights they exercise), along the lines of not being required to divulge the identity of their confidential source (i.e. it would need to create specific rights, as opposed to simply establishing principles). In a related vein, the law would need to include a number of procedural rules, such as about informing those covered by their right not to disclose a source and about how to bring an action for source disclosure before a court.*

FLIP's Pedro Varca Villareal said that while there are already penalties for unlawful surveillance activity in Colombia, "…it could be very interesting to penalise with the particular aim of punishing violations of professional secrecy". But he cautioned about the need for training and education. "Often, professional secrecy tends to be violated by public officials (police or judicial officials). To avoid creating a tension between State powers, this could be implemented if and only if accompanied by training processes (for) officials. In many cases these officials do not understand the scope of the confidentiality of sources and the penalties would be disproportionate without previous pedagogical exercises accompanying them".

2. Other principles emerging from the thematic study underpinning this research

a. Desirability of explicit referencing of source protection in constitutional and nationally-applicable law

Former Special Rapporteur with the Inter-American Commission on Human Rights Catalina Botero made the point that constitutional protection of journalists' sources is desirable "… having this in the constitution is good … because you need a very clear instruction for the judicial power not to do things that can threaten journalism, for example allowing the state to spy on journalists".

This was a view echoed by Australian Constitutional Law expert, Professor George Williams. Given the absence of solid constitutional protections for freedom of expression, or an over-riding piece of legislation at the Federal level in Australia, the introduction of new laws pertaining to data retention and the criminalisation of aspects of national security reporting have alarmed him with respect to source protection:

> *…what we need is not only specific defences but a more generic statute or protection that applies to journalist rights and freedom of speech more generally. ... Given we do not have a bill of rights, and probably aren't getting one soon, an alternative would be…a federal statute that specifically provides for those rights that would be used to trump, or at least interpret other statutes.*

b. Recognition that metadata should also be treated as confidential information by third parties and State actors

Metadata can be used to pinpoint journalists' interactions with their sources even when, for example, the contents of emails or telephone conversations may remain secret.

Digital communications lawyer Leanne O'Donnell commented:

> *A lot of the privilege laws concentrate on the content, whereas what we've learned over the last couple of years is that just as invasive or revealing is the data around that content – the fact that you looked at 'x' websites and you called that phone number and the time you did those things. The data that sits around communications can be just as revealing about patterns and associations, relationships and identity. I think we are going to get to the stage where we are going to have to really grapple with how we protect that data as much as the content.*

c. Transparency clause proposed

Although this issue is partially covered under draft principle 7 above, ("Define an independent judicial process, with appeal potential, for authorised exceptions"), some respondents wished to push it further. For example, Alan Rusbridger proposed a transparency provision whereby journalists are informed when there is a request from authorities to access their data. "… (I)f they're going to go and look at journalists' material then they have an obligation to tell the journalist… a policeman might not be the best judge of whether something imperils a source".

Indicative of the difficulty around the issue is the argument of the former British Transport Police chief constable Andy Trotter, who spoke at a City University London debate in March 2015. He rejected the suggestion that news organisations should be given the opportunity to argue the case against the disclosure of journalists' call records. "If one is investigating a journalist, it is like we are investigating any potential criminal – we don't normally notify them that's what we are going to do (Ponsford 2015b). A similar point was made during the debate by former senior civil servant Sir David Omand, who was involved in drafting the Regulation of Investigatory Powers Act (RIPA) surveillance legislation. He said he believed there was no possibility of notifying journalists about requests to view their phone records, in part because foreign spies often pose as journalists.

On the other hand, there is a distinction between investigating a journalist who is doing his or her job, and investigating a third party. It is also evident that even in the absence of transparency in certain cases, there can still be rules that place limits on the requisitioning of data, and there can still be a form of adversarial framing built into the process.

d. Shield individuals engaged in acts of journalism from targeted surveillance, data retention and handover, and data pertaining to their work netted by mass surveillance (other than in very narrowly defined exceptional circumstances).

Alan Rusbridger urged such protections, as did Australian digital communications lawyer Leanne O'Donnell. But she also acknowledged the practical challenges of implementation: "…it would require those law enforcement agencies to do the right thing because…on a practical level, the ISP who is receiving that request is not going to know that Joe Boggs is a journalist, or that Joe Bloggs is a source. So it would require the law enforcement agency not to make those requests in those categories of communications".

Privacy International's Thomas Falchetto pointed to international examples where such limitations and exemptions are in effect, although only a few countries specifically limit the use of surveillance to identify sources or other protected materials. "The Belgian Law on Protection of Journalists' Sources prohibits the use of 'any detection measure or investigative measure' of any protected media person, unless it is authorised by a judge under the same restrictions as are required to compel a journalist to reveal her source of information". Falchetto made reference to the Council of Europe (CoE) Committee of Ministers 2000 recommendation on 'The Right of Journalists Not to Disclose Their Sources of Information', which deals with journalistic exclusions regarding surveillance and data retention. According to this, Principle 6 (Interception of communication, surveillance and judicial search and seizure) states:

> *a. The following measures should not be applied if their purpose is to circumvent the right of journalists, under the terms of these principles, not to disclose information identifying a source:*
>
> *i. interception orders or actions concerning communication or correspondence of journalists or their employers,*
>
> *ii. surveillance orders or actions concerning journalists, their contacts or their employers, or*
>
> *iii. search or seizure orders or actions concerning the private or business premises, belongings or correspondence of journalists or their employers or personal data related to their professional work.*
>
> *b. Where information identifying a source has been properly obtained by police or judicial authorities by any of the above actions, although this might not have been the purpose of these actions, measures should be taken to prevent the subsequent use of this information as evidence before courts, unless the disclosure would be justified under Principle 3.*

The CoE Principle 3 referred to here defines parameters around to the right of non-disclosure. It specifies that in determining whether a legitimate interest in a disclosure outweighs the public interest in not disclosing information identifying a source, the competent authorities should pay particular regard to the importance of the right of non-disclosure and the pre-eminence given to it in the case-law of the European Court of Human Rights. A disclosure should only be ordered if there is "an overriding requirement in the public interest and if circumstances are of a sufficiently vital and serious nature". Principle 3 further states that the disclosure of information identifying a source should not be deemed necessary unless it can be convincingly established that reasonable alternative measures to the disclosure do not exist or have been exhausted by the persons or public authorities that seek the disclosure.

However, Toby Mendel opposed the inclusion of a principle in the draft framework that would exempt journalists from surveillance or data retention provisions, saying this was neither possible nor reasonable. "Source protection has never been understood as protecting journalists against ordinary criminal law processes, and it would not be justifiable to suggest this. Given the broad nature of any reasonable definition of a journalist, if we were to protect them against surveillance, anyone who wished to engage in terrorist activity could easily bring themselves within that definition. Rather than look at it from this angle, I think the proper solution, at least in democracies, is to enhance the legal and oversight controls over surveillance".

The issue that emerges from this discussion concerns the feasibility and desirability of not intercepting or collecting private journalistic data (or metadata), as well as the distinct issue of limitations on the use of the data that is collected so as to ensure a high level of confidentiality and protection. The general principle, however, maintains protection of confidentiality of sources for acts of journalism as an aspiration in relation to both targeted surveillance and mass surveillance, as well as data retention and rendition, and it points to the value of legal process and narrow conditions being required if confidentiality is to be legitimately compromised.

e. Complementarity of source protection laws with whistleblower legislation

Many of the experts interviewed indicated the need for recognition of parallel whistleblower laws to strengthen the legal framework for source protection. "In the places where we don't have them, we should start with that. And, it's not specifically journalists' protections, but more broadly whistleblower protections, because whistleblower protection laws do help," Javier Garza said.

Henry Maina said: "…if the sources understand that there is protection of whistleblowers, then those two would go hand-in-hand. Where journalists are seeking to have protection of their sources, the best point of entry is to have whistleblower protection, as opposed to making arguments as journalists". He added: "When you begin to think of it as whistleblowers are protected, then you can, as a person who has received this information, seek protection of your source".

However Josh Stearns expressed reservations: "In an ideal world where a whistleblower law was written to include whistleblowing to the press, it could work. But where the rubber meets the road I have a hard time seeing that actually play out in practice. …I also think that there may be philosophical and legal distinctions to be made between the protection of a journalist to gather and disseminate news, versus the rights of someone to reveal wrongdoing that they are witnessing".

f. The need for source protection laws to apply across all mediums

All of the interviewees agreed that source protection laws needed to explicitly encompass digital media to avoid emerging disparities that have resulted in analogue data (e.g. reporters' notepads) being protected, while digital data (e.g. a journalist's hard drive or smartphone) is not protected. "Traditionally when we have thought about how to protect sources, especially in law through things like shield laws, it's been very analogue in focus, and the new world that we live in - in terms of digital surveillance and security - makes a lot of those shield laws problematically dated in some ways," Josh Stearns said.

g. The need to revise existing laws

The Media Legal Defence Institute's Peter Noorlander called for amendments to existing legal frameworks, along with strategic litigation, to ensure their effectiveness in the digital era:

> *Existing national security and search and seizure laws should be amended to strengthen source protection, and it should be made clear in those countries where it is not yet (the case) that source protection is part and parcel of the constitutional right to freedom of expression. Currently this is the case only in European countries, and even there constitutional source*

protection is being undermined, so this will be a large task and take some sustained and combined effort of lobbying and strategic litigation.

Silvia Higuera said that States needed to be convinced to give journalists working in digital environments "the same protection they had in the other mass media".

This was a point also made by one respondent to the survey attached to this Study. Sudanese journalist Liemia Eljaili Abubkr said that source protection laws should be revised to "include articles protecting journalists on the Internet (to ensure that they are not subjected to) criminal punishment" (Abubkr 2014). She also called for the criminalisation of "hacking, spying, filtering and following journalists' communication".

h. Internationally relevant actions

Several interviewees promoted the idea of international-level legal support for source protection. FLIP's Pedro Varca Villareal was among them:

In our opinion these issues are easier to promote if they have international support at the level of a treaty, commemoration in the form of an international day, or the creation of recommendations. It may also have a greater impact if this issue, among others related to fundamental rights on the Internet, were included in exercises such as the Universal Periodic Review of the Human Rights Committee of the United Nations.

Charles Tobin said that treaties and conventions can be very helpful to furthering an international culture where free speech is valued. Bolivian investigative journalist Ricardo Aguilar highlighted the interdependence of secure source protection and development: "Considering the undeniable fact that the confidentiality of the source is a key for access to information and freedom of the press, then its protection far exceeds the mere defence of democratic values and inclusively involves the development of countries".

i. The need to educate civil servants, law enforcement agents and the judiciary in the purpose and value of legal source protection frameworks:

As he argued for in the case of draft principle 8 above, Pedro Vaca Villareal highlighted the importance of including in a framework whether there are measures for promotion, training and awareness, especially with the judiciary and law enforcement. The main problem he said "is the lack of knowledge of legislators and judges regarding the impact of technological surveillance. Beyond these policy changes, it is essential that policies and awareness training of staff are included".

3. Revised 11 Principles for assessing legal source protection frameworks internationally

The following principles represent the research-informed augmentation and expansion of the eight-framework principles originally proposed for expert review, taking into account the feedback of the experts. Accordingly, a robust and comprehensive source protection framework would encompass the need to:

1. Recognise the value to the public interest of source protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country's constitution and/or national law,

2. Recognise that source protection should extend to all acts of journalism and across all platforms, services and mediums (of data storage and publication), and that it includes digital data and meta-data,

3. Recognise that source protection does not entail registration or licensing of practitioners of journalism,

4. Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection,

5. Affirm that State and corporate actors (including third party intermediaries), who capture journalistic digital data must treat it confidentially (acknowledging also the desirability of the storage and use of such data being consistent with the general right to privacy),

6. Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources,

7. Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard,

8. Define exceptions as needing to conform to a provision of "necessity" and "proportionality" — in other words, when no alternative to disclosure is possible, when there is greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible,

9. Define a transparent and independent judicial process with appeal potential for authorised exceptions, and ensure that law-enforcement agents and judicial actors are educated about the principles involved,

10. Criminalise arbitrary, unauthorised and willful violations of confidentiality of sources by third party actors,

11. Recognise that source protection laws can be strengthened by complementary whistleblower legislation.

Further research could develop a repository of examples of model laws and exemplar judgements that address the issues of 'exceptions' and 'necessity' provisions. A summary of such could be appended to this model assessment framework.

8. Gender Dimensions Arising

Women journalists face additional risks in the course of their work – on and offline. In the physical realm, these risks can include sexual harassment, physical assault and rape. In the digital sphere, acts of harassment and threats of violence are rampant. Similarly, female sources face increased risks when acting as whistleblowers or confidential informants.

These issues manifest in several ways as regards the issue of source protection in the digital era:

1. Women journalists face greater risks in dealing with confidential sources
2. Women sources face greater physical risks in encounters with journalists and in revealing confidential information
3. The physical risks confronted by women journalists and sources in the course of confidential communications may require reliance on digital communications
4. Secure digital communications defences, including encryption, are arguably even more necessary for female journalists and sources

Specific factors for consideration

1. Female journalists and sources need to be able to communicate digitally

Female journalists working in the context of reporting conflict and organised crime are particularly vulnerable to physical attacks, including sexual assault, and harassment. In some contexts, their physical mobility may be restricted due to overt threats to their safety, or as a result of cultural prohibitions on women's conduct in public, including meeting privately with male sources. Therefore, women journalists need to be able to rely on secure non-physical means of communication with their sources.

Women sources may face the same physical risks outlined above – especially if their journalistic contact is male and/or they experience cultural restrictions, or they are working in conflict zones.

Additionally, female confidential sources who are domestic abuse victims may be physically unable to leave their homes, and therefore be reliant on digital communications.

These factors present additional challenges for women journalists and sources, in regard to maintaining confidentiality in the digital era.

2. Digital safety and security are paramount for both female journalists and sources

Women journalists need to be able to rely on secure digital communications to ensure that they are not at increased risk in conflict zones, or when working on dangerous stories, such as those about corruption and crime. The ability to covertly intercept and analyse journalistic communications with sources increases the physical risk to both women journalists and their sources in such contexts. Encrypted communications and other defensive measures

are therefore of great importance to ensure that their movements are not tracked and the identity of the source remains confidential.

The risks of exposure for confidential sources are magnified for female whistleblowers. Therefore, they need to be able to have access to secure secure digital communications methods to ensure that they are at minimum risk of detection and unmasking. They also need to have confidence in the ability to make secure contact with journalists to ensure that stories affecting women are told – secure digital communications can be an enabler for women's participation in public interest journalism. They can also help to avoid magnifying the 'chilling' of investigative journalism dependent upon female confidential sources. Also needed are strong legal protections for confidentiality, which are applied in a gender-sensitive manner - especially in regard to judicial orders compelling disclosure.

3. Online harassment and threats

Journalists and sources using the Internet or mobile apps to communicate face greater risk of gendered harassment and threats of violence. These risks need to be understood and mitigated to avoid further chilling women's involvement in journalism – as practitioners or sources.

4. Summary

Strong source protection laws which respond to the challenges of the digital age discussed at length in this Study can help to avoid the chilling of women's involvement in investigative journalism that is dependent upon confidential sources. They can assist in empowering women's participation in accountability reporting that addresses social and development needs, such as systemic failures in public utilities and services, corruption and organised crime.

9. Protecting Journalism Sources in the Digital Age: Conclusion

The legal frameworks that support protection of journalists' sources - at international, regional and country levels - are under significant strain in the digital era. In many of the countries studied, frameworks are being affected by national security, anti-terrorism and data retention legislation that overrides source protection laws, or they risk being undercut by arbitrary surveillance and mass surveillance (Hughes 2012; Learner & Bar Nissim 2014). Other threats arise due to pressure being applied to third party intermediaries to release data that risk exposing sources. There are also increasing challenges to technical measures that support confidentiality, such as limits on anonymity, and moves to outlaw encryption.

Furthermore, there is the question of entitlement to protection: in an era where citizens and other social communicators have the capacity to publish directly to their own audiences, and those sharing information in the public interest are recognised as legitimate journalistic actors by the United Nations, to whom should source protection laws apply? On the one hand, broadening the legal definition of 'journalist' to ensure adequate protection for citizen reporters (working on and offline) is desirable, and case law is catching up gradually on this issue of redefinition. However, on the other hand, it opens up debates about licensing and registering those who do journalism and who wish to be recognised for protection of their sources. This is why the key tests in contemporary society for access to source protection laws are evolving towards the definition and identification of 'acts of journalism', rather than occupational or professional descriptors.

Journalists and news organisations are in the process of adapting their practices – strengthening digital security and reverting to pre-digital era methods of communication with confidential sources. But unless individual States and regional bodies revise and strengthen their legal source protection frameworks, journalists adapting reporting methods and reverting to analogue 'basics' (an option not always practically feasible, especially, as argued above, for many of the women who do journalism) will not be enough to preserve source protection in the digital age. In an era of technologically advanced spy-craft, it is also necessary for States to review surveillance practises and oversight in line with UN General Assembly resolutions on privacy. In addition, source confidentiality requires limits to data retention and rendition laws, improved accountability and transparency measures (applied to both states and corporations in regard to journalistic data), and exemptions for journalistic acts in relation to over-riding national security legislation.

This study has shown that the issue of the confidentiality of journalism sources in the digital age is at the nexus of many intersecting issues. This situation calls out for revision of existing dispensations, and the introduction of new ones, and an 11-pointframework has been advanced to assist in the process. If attention is not given to the new complexities, the institution of source confidentiality will face increasing risks with the deepening of the digital age.

10. Recommendations

At UNESCO, Member States could:

1. Consider framing an explicit resolution that calls on Member States to review and update (as necessitated) their legal frameworks for journalistic source protection drawing on the framework proposed in Thematic Study 3 to ensure their efficacy in the digital era

2. Request support to Member States who wish to adopt and/or review legal frameworks for protecting the confidentiality of journalistic sources in the new conditions

3. Assess source confidentiality issues in submissions to the Universal Periodic Review of the UN Human Rights Committee

4. Support regional workshops, in collaboration with media and civil society, designed to equip digital communicators and journalistic actors with knowledge, skills and the opportunity to collaborate on the challenges and solutions to the issues raised in this study, with regard to continuing investigative journalism practice

5. Consider, where requested, to use this study to help support training of the judiciary, police and civil servants within Member States to ensure that they are adequately educated about the value of legal source protection frameworks.

Individual member States could consider:

1. Applying the proposed framework in Thematic Study 3 above, assessing their own legal source protection dispensations against its provisions

2. Legislating for source protection that extends to digital communications and publishing, and to all acts of journalism in the public interest

3. Ensuring that legislation designed to address national security and crime concerns does not override source protection laws other than in narrowly defined exceptional circumstances

4. Ensuring that surveillance (mass and targeted), and mandatory data retention policies do not undercut legal source confidentiality protection frameworks

5. Working with journalists' organisations and civil society groups to monitor the impacts of the potential corrosive effects on source protection identified in this Study, especially in order to ensure that investigative journalism dependent upon confidential sources is able to continue

6. Consider the applicability of good international practice, including, for instance, the Council of Europe Parliamentary Assembly Recommendation 1950 on the protection of journalists´ sources (CoE 2011) which encourages states to:

- *Legislate for source protection*

- *Review their national laws on surveillance, anti-terrorism, data retention, and access to telecommunications records*

- *Co-operate with journalists' and media freedom organisations to produce guidelines for prosecutors and police officers, and training materials for judges on the right of journalists not to disclose their sources.*

- *Develop guidelines for public authorities and private service providers concerning the protection of the confidentiality of journalists' sources in the context of the interception or disclosure of computer data and traffic data of computer networks*

- *Applying source protection regimes and defined exceptions in a gender-sensitive way*

Recommendations for media actors and other producers of journalism:

1. Engage with digital issues impacting on source confidentiality protection, and actively campaign for laws and rules that provide adequate protection

2. Explain to the public what is at stake in the protection of source confidentiality, especially in the digital age

3. Ensure that sources are aware of the digital era threats to confidentiality

4. Consider altering practices – including 'going back to analogue methods' when required (recognising this may not always be possible due to international or gender dynamics) – in order to offer a degree of protection to their confidential sources

5. Help audiences become more secure in their own communications, for example explaining how encryption works, and why it is important not to have communications security compromised

6. Consider providing technical advice and training to sources to ensure secure communications, with the assistance of NGOs and representative organisations

7. In the case of media leaders, ensure that they also respect their journalists' ethical commitment (and in some cases legal obligation) to source confidentiality

8. In the case of media owners, ensure that their journalists, and freelancers who contribute investigative reports, have access to the appropriate tools and training needed to ensure that they are able to offer the most secure channels of digital communication possible to their sources

Recommendations for civil society

1. Advocate, for robust source protection frameworks in line with that described in Thematic Study 3 above

2. Invest in, and partner with, news publishers and academia to research and develop new tools to aid secure digital communication between journalistic actors and their sources

3. Assist in training and implementation of digital security tools among journalistic actors and whistleblowers

4. Work with UNESCO and other UN actors and Governments to develop complementary whistleblower regimes

5. Assisting in training in digital source protection solutions for both journalists and their sources

General recommendations for multiple stakeholders

1. There should be further research into the impacts of the digital era on source protection in Member States which are not included in this Study's methodological approach

2. Consideration could be given to bi-annual source protection research mapping exercises to build on, and maintain the relevance of, this benchmark global study

3. An international conference/symposium could be convened on the implications of the digital age for legal source protection frameworks internationally

4. There should be further research to develop a repository of examples of model laws and exemplar judgements that address the issues of 'exceptions' and 'necessity' provisions. A summary of such could be appended to the model assessment framework, as identified as desirable in Thematic Study 3.

5. Support should be given to developing an online repository for the specific purpose of making centrally available data on legal and environmental challenges to source protection efficacy within Member States. This could be orchestrated collaboratively with a range of civil society groups via a crowd-mapping exercise

References

Abbas R 2013, 'Proposed Sudan media law targets press freedom' *Al Monitor*, 17 January, viewed 27 February 2015, accessed at: http://www.al-monitor.com/pulse/originals/2013/01/sudan-press-freedom.html

ABC NEWS 2014, 'Schapelle Corby: Federal Court quashes warrants for AFP raid on seven' *ABC News*, 4 April, accessed at: http://www.abc.net.au/news/2014-03-26/schapelle-corby-federal-court-rules-seven-raid-warrants-invalid/5346758

Abouzeid, R (2015) Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

Abdulla, Dr. R (2015) Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

Abubkr, L E, 'Online surveillance and censorship in *Sudan' Association for Progressive Communications*, March, accessed at: http://www.apc.org/en/blog/online-surveillance-and-censorship-sudan.

Ackerman S 2015, 'Back from the dead: US officials to ask secret court to revive NSA surveillance,' *The Guardian*, 3 June, accessed at: < http://www.theguardian.com/us-news/2015/jun/03/nsa-surveillance-fisa-court>

ACLU 2008 Amnesty International et al V Clapper et al 2008, complaint particulars https://www.aclu.org/files/pdfs/natsec/amnesty/07_10_2008_Complaint.pdf)

ACLU et al V Clapper et al Judgement, 2014 https://www.aclu.org/sites/default/files/field_document/clapper-ca2-opinion.pdf)

Act 18 Regulation of Interception of Communications Act 2010, ACTS SUPPLEMENT No. 7 to The Uganda Gazette No. 53 Volume CIII dated 3rd September, 2010, September 3, accessed at: http://www.ulii.org/ug/legislation/act/2010/18/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf Act 747, *Securities Offences (Special Measures) Act 2012* (Malaysia), accessed at: http://www.federalgazette.agc.gov.my/outputaktap/20120622_747_BI_Act%20747%20BI.pdf

Act No.1 of 2013, *The Gazette of Pakistan* 22 February, accessed at: http://www.na.gov.pk/uploads/documents/1361943916_947.pdf

Act on Protection of Specially Designated Secrets, Act No. 108 of 2013 article 22(2) Accessed 25 November 2014 at: http://www.japaneselawtranslation.go.jp/law/detail/?id=2231&vm=04&re=02

Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Parliament of Australia*, accessed at: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report>

Ahmed, R 2015 Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

al Eman, M (2015) Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

Aliaksandrau, A, & Bastunets, A, 2014, *Belarus: Laws and regulations stifle independent media*, Index of Censorship, February 12, accessed at: http://www.indexoncensorship.org/2014/02/belarus-legal-frameworks-regulations-stifle-new-competitors/

Algeria, 2012. *Organic Law N° 12-05 of 12 January 2012 relative to media*. People's Democratic Republic of Algeria. Ministry of Communication. Accessed at: http://www.ministerecommunication.gov.dz/en/node/455

Alves R 2014, 'Trends in global collaborative journalism', *Trends in Newsrooms* 2014, pp.83 -87.

Amnesty International, 2012. "UA 203/12 Sudan – Sudanese youth activist at risk of torture". Accessed at: http://www.amnesty.se/engagera-dig/agera/aktuella-blixtaktioner/ua-20312-sudan-sudanese-youth-activist-at-risk-of-torture/

Amnesty International 2015a, "Amnesty International USA Joins ACLU, Wikimedia in Lawsuit to Stop Mass Surveillance Program" *Amnesty USA*, March 10, accessed at: <http://www.amnestyusa.org/news/press-releases/amnesty-international-usa-joins-aclu-wikimedia-in-lawsuit-to-stop-mass-surveillance-program>

Amnesty International 2015b, "UK surveillance Tribunal reveals the government spied on Amnesty International," *Amnesty International*, 1 July, accessed at: https://www.amnesty.org/latest/news/2015/07/uk-surveillance-tribunal-reveals-the-government-spied-on-amnesty-international/

Anderson D 2015, "A question of trust: Report of the investigatory powers review," Williams Lea Group, June, accessed at: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>

Andrejevic 2014, WikiLeaks, Surveillance, and Transparency, *International Journal of Communication*, 8, pp. 2619–2630

Antiterrorism Proclamation 2009 (Ethiopia) accessed at: http://www.refworld.org/docid/4ba799d32.html

Aregawi, A (2015) Qualitative interview conducted by Federica Cherubini for UNESCO Internet Study: Privacy and Journalists' Sources

Article 16, N°1/11 2013, Governing the Press in Burundi, amending the law N°1/025, accessed at: <http://www.presidence.bi/spip.php?article3779# >

ARTICLE 19 2010, 'Memorandum on the Press and Journalist and the Press and Journalist (Amendment) Bill, 2010 of Uganda', March 2010, *ARTICLE 19* London, accessed at: http://www.article19.org/data/files/pdfs/analysis/uganda-memorandum-on-the-press-and-journalist-act-and-the-press-and-journali.pdf

ARTICLE 19 2010b, Comment on Anti-Terrorism Proclamation, 2009, of Ethiopia, March, accessed at https://www.article19.org/data/files/pdfs/analysis/ethiopia-comment-on-anti-terrorism-proclamation-2009.pdf

ARTICLE 19 2012, 'The Gambia: Analysis of Selected Laws on Media,' ARTICLE 19, 17 April, p 20, accessed at: <http://www.article19.org/data/files/medialibrary/3043/12-04-17-LA-gambia.pdf> & <http://www.article19.org/resources.php/resource/3043/en/the-gambia:-analysis-of-selected-laws-on-media>

ARTICLE 19 2012, 'Article 19 submits brief to Indonesian Constitutional Court on national security and freedom of expression', *ARTICLE 19*, 3 May, accessed at: http://www.article19.org/resources.php/resource/3087/en/article-19-submits-brief-to-indonesian-constitutional-court-on-national-security-and-freedom-of-expression

ARTICLE 19 2013a, "Kenya: Journalists harassed for showing army looting during Westgate mall attack," *ARTICLE 19*, 24 October, accessed at: http://www.article19.org/resources.php/resource/37311/en/kenya:-journalists-harassed-for-showing-army-looting-during-westgate-mall-attack

ARTICLE 19 2013b Rwanda Media Law Does Not Go Far Enough http://www.article19.org/resources.php/resource/3665/en/rwanda:-media-law-does-not-go-far-enough#sthash.8hU72VDz.dpuf

ARTICLE 19 2014 Tajikistan Media Law : Legal Analysis https://www.article19.org/data/files/medialibrary/37717/Tajik_Media-Law_Final-.pdf

ASEAN 2012, ASEAN HUMAN RIGHTS DECLARATION, November, accessed from http://aichr.org/documents/;

Associated Press 2012, 'Sri Lanka arrests 9 web site journalists' *The New York Times*, 29 June, accessed at: http://www.nytimes.com/2012/06/30/world/asia/sri-lanka-arrests-9-web-site-journalists.html?_r=0

Assemblée Nationale (a), 2013, France, *Projet de loi renforçant la protection du secret des sources des journalistes*, accessed at: http://www.assemblee-nationale.fr/14/projets/pl1127-ei.asp

Assemblée Nationale (b), 2013, France, *Projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, accessed at: http://www.assemblee-nationale.fr/14/ta/ta0251.asp

Attanasio 2015 'Will Mexicoleaks Unearth Corruption?' *Latin Times* http://www.latintimes.com/mexican-wikileaks-launched-will-mexicoleaks-unearth-corruption-301638

Auletta K 2013, 'Freedom of Information,' *The New Yorker*, 7 October, viewed 27 February 2015, accessed at: http://www.newyorker.com/magazine/2013/10/07/freedom-of-information

Australian Border Force Bill 2015 (Commonwealth), accessed at: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5408

Axberger, Hans-Gunnar (2015) Interview conducted by Caroline Hammarberg for *Protecting Journalism Sources in the Digital Age*.

Bachmann, I 2010, *Salvadoran congress approves public information access law*, Knight Centre, December 6, accessed at: https://knightcenter.utexas.edu/blog/salvadoran-congress-approves-public-information-access-law

Bacon, W 2015 Qualitative interview conducted by Marcus O'Donnell for UNESCO Internet Study: Privacy and Journalists' Sources

Baitarian L 2015, 'Sudan passes freedom of information law but journalists remain wary' *Committee to Protect Journalists*, 5 February, accessed at: http://cpj.org/blog/2015/02/sudan-passes-freedom-of-information-law-but-journa.php

Baker & McKenzie N.d., 'Further steps against corruption – New whistleblowing regulation in Hungary', viewed 27 February at: <http://bakerxchange.com/rv/ff0013e19dc6b42f64fc91b8f34bafc18da7be67>

Baddour, D 2014, 'Bolivian court demands journalists disclose sources or face 30 years in jail,' *Journalism in the Americas*, Knight Center University of Texas Austin, 11 July, accessed at https://knightcenter.utexas.edu/blog/00-15678-bolivian-court-demands-journalists-disclose-sources-or-face-30-years-jail

Ball J 2015, 'GCHQ captured emails of journalists from top international media' *The Guardian*, 19 January, viewed 20 February, accessed at: http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post

Banisar D 2008, "Speaking of terror: A survey of the effects of counter-terrorism legislation on freedom of the media in Europe," *Council of Europe*, Media and Information Society Division Directorate General of Human Rights and Legal Affairs Council of Europe, November. Accessed at:<http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf

Banisar, D 2007 *Silencing Sources: An international survey of protections and threats to journalists' sources*, Privacy International, accessed at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1706688 accessed 25/6/2014

Barker Exchange 2014 *Further steps against corruption - New Whistleblowing Regulation in Hungary*. Accessed February 27th, 2015 http://bakerxchange.com/rv/ff0013e19dc6b42f64fc91b8f34bafc18da7be67

Barns G & Newhouse G 2015, 'Border Force Act: detention secrecy just got worse,' *Australian Broadcasting Corporation*, 27 May, accessed at: http://www.abc.net.au/news/2015-05-28/barns-newhouse-detention-centre-secrecy-just-got-even-worse/6501086

Baron, M (2015) Qualitative interview with Marty Baron conducted by Julie Posetti for *Protecting Journalism Sources in the Digital Age*. Barseghyan A 2014, 'Legal Precedent for News Media to Disclose Source is Detrimental to Freedom of Speech' *Media.am*, 12 September, viewed 27 February at http://media.am/en/armenian-journalist-info-source-case-in-court

Bartlett QC, P 2015 Qualitative interview conducted by Marcus O'Donnell for UNESCO Internet Study: Privacy and Journalists' Sources

Basille O 2009, 'Bulgaria - Resignation or resistance, Bulgaria's embattled press hesitates', *Reporters Sans Frontieres (RSF)*, January, accessed at: http://en.rsf.org/IMG/pdf/rsf_rep_bulgaria_en.pdfBasson A 2009, 'Very brave for a young man' Mail & Guardian, 22 May, accessed at: http://mg.co.za/article/2009-05-22-very-brave-for-a-young-man

Balev K 2013, 'UPDATE: Nigeria journalists freed - Pair must continue to check in with police,' *International Press Institute*, 21 July, accessed at: http://www.freemedia.at/newssview/article/update-nigeria-journalists-freed.html

BBC 2011, 'Malaysia to scrap Internal Security Act' *BBC* 15 September, accessed at: http://www.bbc.co.uk/news/world-asia-pacific-14937820;

BBC 2013a, 'Uganda's Daily Monitor reopens after police closure' *BBC* 30 May, Accessed at: http://www.bbc.com/news/world-africa-22717291.

BBC 2013b, 'Westgate attack: Kenya CCTV 'shows soldiers looting", *BBC*, October 21, accessed at: http://www.bbc.com/news/world-africa-24606152

BBC News 2014 Andy Coulson jailed for 18 months over phone hacking, *BBC News Online*. Accessed: http://www.bbc.com/news/uk-28160626

BBC 2015a "MPs win surveillance powers legal challenge," *BBC*, 17 July, accessed at: http://www.bbc.com/news/uk-politics-33564442

BBC 2015b 'Operation Elveden: Budget leaker Jonathan Hall avoids jail', *BBC Online*, Available: http://www.bbc.com/news/uk-31169254

BBC News Middle East, 2011, Syria Protests: Assad to Lift state of emergency, 20 April, accessed at: http://www.bbc.co.uk/news/world-middle-east-13134322

Bauman, Zygmunt et al., 2014, 'After Snowden: Rethinking the Impact of Surveillance,' *International Political Sociology*, 8:2, 121–140

Bauer N 2012, 'Bosasa loses source case appeal bid against M & G – with costs,' *Mail & Guardian*, 22 November, accessed at: http://mg.co.za/article/2012-11-22-bosasa-lose-source-case-appeal-bid-with-costs

Benavente, C (2015) Qualitative interview conducted by Alice Matthews for UNESCO Internet Study: Privacy and Journalists' Sources

Berglund-Sigbahn, K (2015) Qualitative interview conducted by Angelique Lu for UNESCO Internet Study: Privacy and Journalists' Sources

Best C 2010, 'More on Wigmore in R v. National Post (2010)' *The Court, York University*, 21 May, viewed 27 February at http://www.thecourt.ca/2010/05/21/more-on-wigmore-in-r-v-national-post-2010/

Bigo et al 2013 *National Programmes for Mass Surveillance of Personal Data in EU Member States and their compatibility with EU Law*, European Parliament http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf

Bhatia G 2015, "State Surveillance and the Right to Privacy in India: A Constitutional Biography" May 12 , 26(2) National Law School of India Review 127 (2014); Accessed at: http://ssrn.com/abstract=2605317

Blomberg M, Wilwohl J & Ana P 2014, 'Police inspected telecom firms' routers, records,' *Cambodia Daily*, 9 December, accessed at: https://www.cambodiadaily.com/news/police-inspected-telecom-firms-routers-records-73833/

Blue V 2014, " Top gov't spyware company hacked; Gamma's FinFisher leaked," *Zero Day*, 6 August, accessed at: http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked/

Borger J 2013. 'NSA files: why the Guardian in London destroyed hard drives of leaked files', *The Guardian*, August 20, accessed at: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

Bosasa Operation (Pty) Ltd v Basson and Another 09/29700, accessed at: http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html

Botero, C, 2012, *Annual Report of The Inter-American Commission On Human Rights*, Volume II, Report of the Office of the Special Rapporteur for Freedom of Expression

Botero C 2013, "Violence against journalists and media workers: inter-American standards and national practices on prevention, protection and prosecution of perpetrators,' *Office of the Special Rapporteur for Freedom of Expression Inter-American Commission on Human Rights*, 31 December, viewed 27 February 2015, accessed at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_Violence_WEB.pdf

Botero, C 2015 Qualitative interview conducted by Alice Matthews for UNESCO Internet Study: Privacy and Journalists' Sources

Botero Marino, C 2014, "Annual Report of the Inter-American Commission on Human Rights 2013: Annual report of the office of the special rapporteur for freedom of expression,' *volume ii, General Secretariat Organization of American States Washington, D.C*, 22 April, viewed 27 February 2015, accessed: < http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf>

Bowcott, O 2014 David Miranda allowed to appeal against ruling on Heathrow detention, *The Guardian*, May 15, accessed at: http://www.theguardian.com/world/2014/may/15/david-miranda-appeal-high-court-ruling-detention-heathrow

Bowcott O 2015 a, 'UK-US surveillance regime was unlawful for 'seven years,' *The Guardian*, 6 February, viewed 27 February 2015, accessed at: http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa

Bowcott O 2015b, "High court rules data retention and surveillance legislation unlawful," *The Guardian*, 17 July, accessed at: < http://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful>

Brandeisky K 2013, "NSA surveillance lawsuit tracker," *Propublica*, 10 July, accessed at: http://projects.propublica.org/graphics/surveillance-suits

Breemen, K, 2014, 'Dutch legislator proposes two bills on the protection of journalistic sources' *IRIS Merlin*, accessed at: http://merlin.obs.coe.int/iris/2014/10/article26.en.html

Broadcasting and Telecommunications Act 2014 (Mexico), accessed at: http://leftwardthinking.com/wp-content/uploads/2014/04/Decreto_ley_competencias.pdf

Buenos Aires Herald, 2014, '*Happy navel-gazing day*', accessed at: http://www.buenosairesherald.com/article/161445/happy-navelgazing-day

Bureau of Investigative journalism and Alice Ross v. The United Kingdom (2014) 62322/14, *European Court of Human Rights*, communicated 5 January 2015, accessed at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-150946#{%22itemid%22:[%22001-150946%22]}

Burke 2012, 'Shielding the Public Interest: What Canada Can Learn from the United States in the Wake of National Post and Globe & Mail', 35 B.C. *Int'l & Comp. L. Rev.* 189 (2012), accessed at: < http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1668&context=iclr>

Burundi Press Law 2013 Loi N°1/11 Du 4 Juin 2013 Portant Modification De La Loi N°1/025 Du 27 Novembre 2003 Regissant La Presse Au Burundi, Article 16 http://www.presidence.bi/spip.php?article3779

Burundian journalists union v the Attorney General of the Republic of Burundi, Reference No.7 of 2013, accessed at: http://eacj.org/wp-content/uploads/2015/05/Reference-No.7-of-2013-Final-15th-May-2c-2015-Very-Final1.pdf

Cairo Institute for Human Rights Studies 2014, 'Administrative court law suit to stop social media surveillance', *Cairo Institute for Human Rights Studies*, 18 June, accessed at: http://www.cihrs.org/?p=8816&lang=en

Campbell, M 2013), 'Under Cover of Security, Governments Jail Journalists' *Committee to Protect Journalists*, https://www.cpj.org/2013/02/attacks-on-the-press-misusing-terror-laws.php

Caixin (2014) http://opinion.caixin.com/2014-05-12/100675842.html Feb 26, 201

Canadian Journalists for Free Expression 1996, 'Concerns for Press Freedom in Botswana' *Canadian Journalists for Free Expression*, 29 March, accessed at: https://cjfe.org/resources/protest_letters/concerns-press-freedom-botswana

Case 1:10-mj-00291-AK, US District Court 2010, 11 January 2011, accessed at: http://apps.washingtonpost.com/g/page/local/affidavit-for-search-warrant/162/

CECC 2009, *Macau Government Passes Controversial National Security Law*, Congressional Executive Commission on China, 6 November, accessed at: <http://www.cecc.gov/publications/commission-analysis/macau-government-passes-controversial-national-security-law>

Cheema, U (2015) Qualitative interview conducted by Federica Cherubini for UNESCO Internet Study: Privacy and Journalists' Sources

Cherfauoi, Z (2015) Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

Churchill F, 2015, "Under Surveillance: Protecting Journalistic Sources," *Frontline Club London*, July 8, accessed at: <http://www.frontlineclub.com/under-surveillance-protecting-journalistic-sources/>

CIPESA 2014, *State of Internet Freedoms in Uganda 2014: An investigation into the policies and practices defining internet freedom in Uganda*, CIPESA, May, viewed 24 February 2015, accessed at: http://www.cipesa.org/?wpfb_dl=76

CIPESA 2015 'Reflections on Uganda's Draft Data Protection and Privacy Bill 2014,' CIPESA ICT *Policy Briefing Series*, February 2015, viewed 27 February 2015, accessed at: http://www.cipesa.org/?wpfb_dl=102

Citizen Lab Research, 2013 Short Background: Citizen Lab Research on FinFisher Presence in Malaysia, accessed at: https://citizenlab.org/wp-content/uploads/2013/05/shortbg-malaysia1.pdf

Citizen Lab Research 2014 Hacking Team Re-loaded? US-based Ethiopian Journalists Again Targeted With Spyware https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/ Accessed March 10th, 2015

Code de l'Information 2012 (Algeria), Article 85, accessed at: http://www.joradp.dz/TRV/FInfo.pdf

Code of Ethics for Professional Journalists Greece, n.d., viewed 27 February 2015 at: http://ethicnet.uta.fi/greece/code_of_ethics_for_professional_journalists

Colombo Telegraph 2012, 'Sri Lanka Mirror Staffers Arrested And Taken To The Fourth Floor By CID', *Colombo Telegraph*, June 29, accessed at: https://www.colombotelegraph.com/index.php/sri-lanka-mirror-staffers-arrested-and-taken-to-the-fourth-floor-by-cid/

Committee to Protect Journalists (CPJ) 2008, 'Kyrgyzstan: Police raid newspaper, confiscate computers, seal newsroom,' *Committee to Protect Journalists*, 17 June, accessed at: https://cpj.org/2008/06/kyrgyzstan-police-raid-newspaper-confiscate-comput.php

Committee to Protect Journalists (CPJ) 2009, 'Liberian journalist could be forced to reveal source,' *Committee to Protect Journalists*, Feb 3, accessed at: https://cpj.org/2009/02/liberian-journalist-could-be-forced-to-reveal-sour.php

Committee to Protect Journalists (CPJ) 2010, 'Attacks on the Press in 2010: A worldwide survey by the Committee to Protect Journalists', *Committee to Protect Journalists*, United Book Press USA, accessed at: https://cpj.org/attacks_on_the_press_2010.pdf

Committee to Protect Journalists (CPJ) 2011, "Umar Cheema, Pakistan – International Press Freedom Awards", Committee to Protect Journalists, accessed at: https://cpj.org/awards/2011/umar-cheema-pakistan.php Committee to Protect Journalists (CPJ), 2012a, 'In Algeria, new media law stifles free expression', *Committee to Protect Journalists*, January 25, accessed at: http://cpj.org/2012/01/in-algeria-new-media-law-stifles-free-expression.php

Committee to Protect Journalists (CPJ), 2012b, 'Angolan police raid weekly's office, seize computers', *Committee to Protect Journalists*, March 12, accessed at: https://cpj.org/2012/03/angolan-police-raid-weeklys-office-seize-computers.php

Committee to Protect Journalists (CPJ), 2012c, 'Sri Lankan police raid offices of two news websites', *Committee to Protect Journalists*, June 29, accessed at: https://cpj.org/2012/06/sri-lankan-police-raid-offices-of-two-news-website.php

Committee to Protect Journalists (CPJ) 2013, 'Monitor, Red Pepper closures spark protests in Uganda', *Committee to Protect Journalists*, May 29, accessed at: https://cpj.org/2013/05/monitor-red-pepper-closures-spark-protests-in-ugan.php

Committee to Protect Journalists (CPJ) 2014a, 'Argentine authorities raid news outlet and confiscate materials' *Committee to Protect Journalists* 30 October, viewed 27 February 2015, accessed at <http://cpj.org/x/5dd4>

Committee to Protect Journalists (CPJ) 2014b, "Sunday Standard editor Outsa Mokone arrested in Botswana," *Committee to Protect Journalists*, 12 September, accessed at: < https://cpj.org/2014/09/sunday-standard-editor-outsa-mokone-arrested-in-bo.php>

Committee to Protect Journalists (CPJ) 2015a, 'Burundian journalist arrested, charged after not revealing source' *Committee to Protect Journalists*, 21 January, accessed at: https://cpj.org/2015/01/burundian-journalist-arrested-charged-after-not-re.php

Committee to Protect Journalists (CPJ) 2015c, "Ethiopia suspected of spying on independent TV network ESAT," *Committee to Protect Journalists*, 10 March, accessed at: https://cpj.org/2015/03/ethiopia-suspected-of-spying-on-diaspora-tv-networ.php

Computer Crimes Law 2013 (Peru), accessed at: http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc02_2011_2.nsf/d99575da99ebfbe305256f2e006d1cf0/a8851de57eec4e8205257c0c004fc83d/$FILE/30096.pdf

Constitutional Court of Colombia 2009 T-298/09 http://www.corteconstitucional.gov.co/relatoria/2009/T-298-09.htm

Constitution of the Russian Federation 1993, adopted in a national referendum of December 12 1993, (Конституция Российской Федерации, Принята всенародным голосованием 12 декабря 1993 г.) made available by the Official Website of the President of the Russian Federation, accessed at: http://constitution.kremlin.ru/

Constitute Project 2012, 'Dominican Republic's Constitution 2010', *Constitution Project* trans. L F Valle Velasco, accessed at: https://www.constituteproject.org/constitution/Dominican_Republic_2010.pdf

Council of Europe 2007, *Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis*, 1005th meeting, Council of Europe, 26 September, accessed at: https://wcd.coe.int/ViewDoc.jsp?id=1188493

Council of Europe HRC 2011, "Protection of journalists from violence: Issue discussion paper" Council of Europe, accessed at: https://wcd.coe.int/ViewDoc.jsp?id=1899957https://wcd.coe.int/ViewDoc.jsp?id=1899957

Council of Europe 2011, *Recommendation 1950: The protection of journalists' sources*', Parliamentary Assembly - Council of Europe, 25 January accessed at: http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/EREC1950.htm

Council of Europe Committee of Ministers 2000 *Recommendation on 'The Right of Journalists Not to Disclose Their Sources of Information'* http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec%282000%29007&expmem_EN.asp

Court of Justice of the European Union 2014, 'The Court of Justice declares the Data Retention Directive to be invalid' Court of Justice press release, 8 April, viewed 27 February 2015, accessed at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Crook, Tim, 2014, 'Political attack on journalists' sources undermines democracy and must be stopped,' *The Conversation*, 8 October, Available: http://theconversation.com/political-attack-on-journalists-sources-undermines-democracy-and-must-be-stopped-32537

Cruz 2011 *Comisión Luizar violó secreto de comunicación de periodistas* http://archivo.larepublica.pe/03-08-2011/comision-luizar-violo-secreto-de-comunicacion-de-periodistas

Cruz, D, 2014, *Colombian military intelligence hacks communication between journalists and FARC in Cuba*, Knight Centre, February 13, accessed at: https://knightcenter.utexas.edu/blog/00-15136-colombian-military-intelligence-hacks-communication-between-journalists-and-farc-cuba

Cummings 2015 'Wikileaks For Africa' *The Guardian* http://www.theguardian.com/world/2015/jan/13/wikileaks-for-africa-introducing-afrileaks

Cybercrime Prevention Act, 2012, (Philippines) s12, RA 10175, original section accessed at: http://www.gov.ph/2012/09/12/republic-act-no-10175/

Damgé M, Cosnard D 2015, 'La liberté d'informer serait-elle vraiment menacée par le « secret des affaires?' *Le Monde*, 28 January, viewed 27 February accessed at: http://www.lemonde.fr/les-decodeurs/article/2015/01/28/la-liberte-d-informer-serait-elle-vraiment-menacee-par-le-secret-des-affaires_4564985_4355770.html

Danguilan-Vitug, M 2015 Qualitative interview conducted by Angelique Lu for UNESCO Internet Study: Privacy and Journalists' Sources

David Miranda v Secretary of State for the Home Department and Others CO/11732/2013, 18 February 2014, accessed at: < https://www.judiciary.gov.uk/judgments/miranda-v-sosfhd-and-others/>

Davies, Nick, 2014 *Hack Attack: How the Truth Caught Up with Rupert Murdoch*, London: Chatto Windus.

Davis 2014, 'MPs get go-ahead to challenge snooping law', *David Davis*, accessed at: <http://www.daviddavismp.com/david-davis-secures-judicial-review-of-dripa/>

Davis & Watson judgement 2015 (Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014 https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf)

Dawn.com 2013, 'Fair Trial Act' signed into law' *Dawn.com*, 20 February, accessed at: http://www.dawn.com/news/787426/fair-trial-act-signed-into-law

Decree 1129, 2012 (Peru), Article 12, accessed at: http://spij.minjus.gob.pe/clp/contenidos.dll/temas/coleccion00000.htm/tomo00003.htm/libro00004.htm/sumilla00007.htm?f=templates$fn=document-frame.htm$3.0#JD_DLEG1129

Decree 1704, 2012 (Colombia) accessed at: http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/Agosto/15/DECRETO%201704%20DEL%2015%20DE%20AGOSTO%20DE%202012.pdf

Decree No. 10/III Media Act (Timor Leste) Article 2, a), accessed at: http://www.hrw.org/news/2014/07/15/timor-leste-press-law-

Der Spiegel 2010, 'Defending Privacy: German High Court Limits Phone and E-Mail Data Storage,' *Der Spiegel*, 2 March, accessed at: < http://www.spiegel.de/international/germany/defending-privacy-german-high-court-limits-phone-and-e-mail-data-storage-a-681251.html>

Der Spiegel 2013 'Snowden Document: NSA Spied On Al Jazeera Communications,' *Der Spiegel*, 31 August, accessed at: http://www.spiegel.de/international/world/nsa-spied-on-al-jazeera-communications-snowden-document-a-919681.html

Der Spiegel 2015, 'An Attack on Press Freedom: SPIEGEL Targeted by US Intelligence,' *Der Spiegel*, 3 July, accessed at: < http://www.spiegel.de/international/germany/the-nsa-and-american-spies-targeted-spiegel-a-1042023.html>

Devereaux R 2014, 'UK Court: David Miranda detention legal under terrorism law,' *The Intercept*, 19 February, accessed at: < https://firstlook.org/theintercept/2014/02/19/uk-court-david-miranda-detention-legal-terrorism-law/>

Diaz Hernandez, M, 2014, *Venezuela's New Security Agency: Watching the Web With No Judicial Oversight*, March 19, accessed at: http://advocacy.globalvoicesonline.org/2014/03/19/venezuelas-new-security-agency-watching-the-web-with-no-judicial-oversight/

Dibetle M 2010, 'Mthethwa: 'A friend of a criminal is a criminal," *Mail & Guardian*, 21 January, accessed at: <http://mg.co.za/article/2010-01-21-mthethwa-a-friend-of-criminal-is>

Digital Rights Ireland Ltd C-293/12 v Minister for Communications et al Ireland, 8 April 2014 Directive 2006/24/EC, Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, accessed at: http://curia.europa.eu/juris/document/document .jsf?docid=150642&-mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=45461 and http://www.loc.gov/law/help/eu-data-retention-directive/eu-data-retention-directive.pdf

Di Martino RE 2014, 'What the European court condemned, is valid for the Paraguayan Electronic Commerce Act' *Berkemeyer Attorneys & Counsellors*, 18 June, viewed 27 February, accessed at <http://www.lexology.com/library/detail.aspx?g=c4aefeef-705f-48d0-84b8-c758b65b8098 >

Dixon R 2013, 'Ugandan government claims victory in standoff with press' May 30, Accessed at: http://articles.latimes.com/2013/may/30/world/la-fg-wn-uganda-media-20130530

Draft of 20th August 2014, The Data Protection and Privacy Bill of 2014, Arrangement of Clauses, accessed at National Information Technology Authority - Uganda (NITAU): http://www.nita.go.ug/sites/default/files/publications/Draft%20Data%20Protection%20and%20PrivacyBill%20-%20Revised%20PDF.pdf

DOJ 2013 *Report on Review of News Media Policies* http://www.justice.gov/iso/opa/resources/2202013712162851796893.pdfDOJ 2014 Policy Regarding Obtaining Information From, or Records of, the News Media; and Regarding Questioning, Arresting, or Charging of the News Media https://s3.amazonaws.com/s3.documentcloud.org/documents/1020977/final-rule-28-cfr-50-10-ag-order.pdf

Dorling P 2014, 'Australians may pay more for medicines under trade deal' *The Sydney Morning Herald*, 16 October, accessed at: http://www.smh.com.au/national/australians-may-pay-more-for-medicines-under-trade-deal-20141016-1175a2.html

D.R. 2015, 'Why locking up leakers makes sense' *The Economist*, 29 January, viewed 27 February 2015 at: <http://www.economist.com/blogs/democracyinamerica/2015/01/press-freedom-and-national-security >

Duncan J 2014, 'Communications surveillance in South Africa: The case of the Sunday Times newspaper', in *Communications Surveillance in the Digital Age* Global Information Society Watch 2014, accessed at: http://www.giswatch.org/en/country-report/communications-surveillance/south-africa

East Timor Law and Justice Bulletin, 2014, '*East Timor's Court of Appeal rules controversial media law unconstitutional*', 21 August, accessed at: http://www.easttimorlawandjusticebulletin.com/2014/08/east-timors-court-of-appeal-rules.html

Editorial Board, The New York Times 2015, "Overkill on a C.I.A. Leak Case" *The New York Times*, 13 May, accessed at: < http://www.nytimes.com/2015/05/13/opinion/overkill-on-a-cia-leak-case.html>

Egyptian Ministry of Interior 2014, 'Social networks security hazard monitoring project booklet,' *Ministry of Interior*, 1 June, accessed at: http://www.cihrs.org/wp-content/uploads/2014/06/MOI-SNSHM-rfp-June-2014_en.pdf

El Nacional. '*Con el Cesppa el gobierno podra vigilar sin limites*', accessed at: http://www.el-nacional.com/politica/Cesppa-gobierno-podra-vigilar-limites_0_355764628.html

Electronic Frontier Foundation 2011 (EFF), *Freedom Of Expression, Privacy And Anonymity On The Internet*, Electronic Frontier Foundation, January, viewed 24 February 2015, accessed at: https://www.eff.org/Frank-La-Rue-United-Nations-Rapporteur. 24 Feb. 2015.)

Electronic Frontier Foundation (EFF), (no date), *Mandatory Data Retention Around the World: Argentina*, accessed at: https://www.eff.org/issues/mandatory-data-retention/argentin

Electronic Frontier Foundation (EFF), n.d., 'Mass Surveillance Technologies,' Electronic Frontier Foundation. Viewed February 24, 2015, accessed at https://www.eff.org/issues/mass-surveillance-technologies

Electronic Frontier Foundation (EFF) n.d. ' Mapping laws on government access to citizens' data: Columbia', *Electronic Frontier Foundation*, viewed 27 February 2015, accessed at <https://www.eff.org/pages/mapping-laws-government-access-citizens-data-colombia>

Electronic Frontier Foundation (EFF) n.d. '*Success Story: Breaking News About Data Retention*' *Electronic Frontier Foundation*, viewed 27 February 2015, accessed at: <https://www.eff.org/pages/success-story-breaking-news-about-data-retention>

Electronic Frontier Foundation (EFF)/IFEX 2012, 'Media sceptical over Press Council Act amendments' *IFEX*, 3 August, accessed at: http://www.ifex.org/sri_lanka/2012/08/03/press_council_act/

Ellison, Sarah 2012, Murdoch's Civil War, *Vanity Fair*, June http://www.vanityfair.com/news/business/2012/06/rupert-murdoch-trial-news-of-the-world-lawsuit

eNCA 2014, 'Botswana journalist accuses government of repression after fleeing,' *eNCA*, 12 September, accessed at: http://www.enca.com/botswana-journalist-accuses-government-repression-after-fleeing

Endominicana.net, 2012, 'Nuria presenta cuentas bancarias de Félix Bautista, donde reparte millones a políticos 1ra' [online], viewed 27 February 2015, accessed at< https://www.youtube.com/watch?v=qlfOBgMlloc#t=34>

ERDi 2010, 'German Federal Constitutional Court rejects data retention law,' *ERDi*, 10 March, accessed at: <https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/ >

Ermorut F 2013, 'Gov't plans to monitor social media' *New Vision* 31 May, viewed 27 February 2015, accessed at: http://www.newvision.co.ug/news/643403-gov-t-plans-to-monitor-social-media.html

ESIEA Journalists' Union of the Athens Daily Newspapers http://www.esiea.gr/arxes-deontologias/

Espectador.com 2014, 'Caso Gelman: polémica porque juez levantó secreto de prensa,' *Espectador.com*, 19 March, viewed 27 February 2015, accessed at: < http://www.espectador.com/politica/287203/caso-gelman-polemica-porque-juez-levanto-secreto-de-prensa>

EthicNet http://ethicnet.uta.fi/greece/code_of_ethics_for_professional_journalists)

Eubanks, V, 2014, Want to Predict the Future of Surveillance? Ask Poor Communities, *American Prospect*, January 15. Available: http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities

Euractiv, 2010, *Swedish law gives shelter to controversial Wikileaks site*, April 9. Accessed at: http://www.euractiv.com/infosociety/sweden-gives-legal-shelter-controversial-wikileaks-site-news-426138

European Information Society Institute 2014, 'Slovak Constitutional Court Suspends Data Retention Legislation' *EISI*, 24 April. Accessed at: <http://www.eisionline.org/index.php/projekty-m/ochrana-sukromia/74-us-data-retention-suspension>

European Court of Human Rights (ECtHR) 1996 Goodwin v United Kingdom http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57974

European Union (EU) 2015 *Joint Statement of Ministers for the Interior*, European Union https://eu2015.lv/images/news/2015_01_11_Joint_statement_of_ministers_for_interrior.pdf)

European University Institute, Centre for Media Pluralism and Media Freedom, 2014, *Status of European Journalists*, accessed at: http://journalism.cmpf.eui.eu/maps/journalists-status/

European University Institute, N.d., '*Status of European Journalists*', viewed 27 February 2015, <http://journalism.cmpf.eui.eu/maps/journalists-status/>

Evans, M 2012, *What you need to know about Costa Rican Cybercrime Offence Law 9048*, July 18, accessed at: http://news.co.cr/what-you-need-to-know-about-costa-rican-cybercrime-offence-law-9048/10702/

Evidence (Journalists) Amendment Bill 2014, (Australia) *Part 8A, 72*, accessed at: http://www.legislation.sa.gov.au/LZ/B/CURRENT/EVIDENCE%20%28JOURNALISTS%29%20AMENDMENT%20BILL%202014_HON%20STEPHEN%20WADE%20MLC/C_AS%20RECEIVED%20IN%20HA/EVIDENCE%20JOURNALISTS%20AMENDMENT%20BILL%202014.UN.PDF

Evidence Act 1995 Cth, s126G (1), (Australia), accessed at: http://www.legislation.nsw.gov.au/sessionalview/sessional/act/1995-25.pdf

Evidence Act 2001 ACT, s 126J (Australia), accessed at: http://www.legislation.act.gov.au/a/2011-12/current/pdf/2011-12.pdf

Ezieh S, 'Plot to overthrow Biya: Military Tribunal issues travel ban on journalists and bars them from practising,' *Cameroon Journal*, 28 October, accessed at: < http://www.cameroonjournal.com/over-plot-to-overthrow-biya/>

Falchetta, T (2015) Qualitative interview conducted by Emma Goodman for UNESCO Internet Study: Privacy and Journalists' Sources

Farook Thajudeen T. 2012, 'Sri Lanka Mirror case set aside', The Daily FT, September 19, accessed at: http://www.ft.lk/2012/09/19/sri-lanka-mirror-case-set-aside/ Farrell P 2015 a, 'Journalists reporting on asylum seekers referred to Australian police', *The Guardian Australia*, 21 January, accessed at: http://www.theguardian.com/australia-news/2015/jan/22/journalists-reporting-on-asylum-seekers-referred-to-australian-police

Farrell P 2015 b, 'Detention centre staff speak out in defiance of new asylum secrecy laws,' *The Guardian Australia*, 30 June, accessed at: http://www.theguardian.com/australia-news/2015/jul/01/detention-centre-staff-speak-out-in-defiance-of-new-asylum-secrecy-laws

Federal Law on communications N 126-ФЗ, (Russian Federation), adopted July 7 2003 N 126-ФЗ, made available by *Rossiskaja Gazeta (Российская газета),* official newspaper of the Parliament of the Russian Federation, accessed at: http://rg.ru/2003/07/10/svjaz-dok.html

Federal law on surveillance N 144-ФЗ, (Russian Federation), adopted August 12 1995, made available by the official website of the Foreign Intelligence Service (Служба внешней разведки), accessed at: http://svr.gov.ru/svr_today/doc07.htm

Federal Government Gazette Malaysia 2012, 'Appointment of date coming into operation' *Federal Government Gazette* 31 July, accessed at: http://www.federalgazette.agc.gov.my/outputp/pub_20120731_P.U.%20(B)%20256%20-%20Penetapan%20Permulaan%20Kuat%20Kuasa%20-%20SOSMA.pdf;

Ferghana, 2011. "Узбекистан: В ташкентском аэропорту задержана выпускница Академии ОБСЕ и «Немецкой волны» Елена Бондарь" [Uzbekistan: Tashkent airport detained a graduate of the Academy of the OSCE and the "Deutsche Welle" Elena Bondar], Ferghana News, August 22, 2011/ accessed at: http://www.fergananews.com/news.php?id=17166;

Fernandez, J. and Pearson, M. 2015 (forthcoming). Shield laws in Australia – legal and ethical implications for journalists and their confidential sources. Pacific Journalism Review, vol 21, issue 1.

Fernandez, Joseph M., 2014, 'Journalists' confidential sources: Reform lessons from recent Australian shield law cases,' *Pacific Journalism Review*, 20:1, 117-137

Fisher, D 2014 'Dirty Politics: Police Raid Nicky Hager's Home', *New Zealand Herald*, 6 October 2014 accessed at: http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11337913

Fitzsimmons C 2008, 'Shiv Malik ordered to hand police source material for terrorism book,' *The Guardian*, 27 June, accessed at: http://www.theguardian.com/media/2008/jun/27/pressandpublishing.medialaw

Fitzsimons S, Macfarlane K, Khalili M 2014, 'Revealed: the day Guardian destroyed Snowden hard drives under watchful eye of GCHQ – video,' *The Guardian*, 31 January, accessed at: < http://www.theguardian.com/world/video/2014/jan/31/snowden-files-computer-destroyed-guardian-gchq-basement-video>

Free Flow of Information Act of 2013 (US), accessed at: https://www.congress.gov/bill/113th-congress/senate-bill/987/text

Freedom House, 2014 (a), Austria, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/austria#.VHNzfoeBsX

Freedom House, 2014 (b), Burundi, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/burundi#.VGjaC4dhsj4

Freedom House, 2014 (c) Estonia, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/estonia#.VHNpUoeBsXw

Freedom house 2014 (d), Ethiopia, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/ethiopia#.VGm3v1eUewE

Freedom House, 2014 (e) France, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/france#.VGo2g4eBsX

Freedom House, 2014 (f), Indonesia, Freedom of the Press, accessed at: https://www.freedomhouse.org/report/freedompress/2014/indonesia#.VHtp0PTF85s

Freedom House, 2014 (g), Israel, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/israe

Freedom House 2014 (h) Costa Rica https://freedomhouse.org/report/freedom-world/2014/costa-rica#.VbDuhbeAatw

Freedom House 2014 (i), 'Japan' *Freedom House*, accessed at: https://freedomhouse.org/report/freedom-press/2014/japan#.VOz1blPF9A8

Freedom house 2014 (j), South Africa, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-world/2014/south-africa-0#.VHJCSodE1nJ

Freedom house 2014 (k), Sudan, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2014/sudan#.VGnFuFeUewE

Freedom House 2014 (l) Freedom House 2014, 'Belarus' Freedom House, viewed 27 February 2015 at: https://freedomhouse.org/report/freedom-net/2014/belarus

Freedom House 2014 (m) 'Georgia' *Freedom House*, viewed 27 February at <https://freedomhouse.org/report/freedom-net/2014/georgia>

Freedom House 2014 (n) 'Columbia' viewed 27 February 2015, accessed at: <https://freedomhouse.org/report/freedom-net/2014/colombia>

Freedom House, 2013 (a) 'Belarus' viewed 27 February 2015 at <https://freedomhouse.org/report/freedom-net/2013/belarus>

Freedom House 2013 (b) 'Czech Republic', viewed 27 February2015, accessed at: https://freedomhouse.org/report/freedom-press/2013/czech-republic

Freedom House 2013 (c) 'Angola', Freedom of the Press accessed at: < https://freedomhouse.org/report/freedom-press/2013/angola#.VYl6J-dCVRk

Freedom House 2013 (d), Ecuador, Freedom of the Press, accessed at: http://www.freedomhouse.org/report/freedom-net/2013/ecuador#.VFjh8edE1nI

Freedom House 2013 (e), Germany, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2013/germany#.VGhyAYdhsj4

Freedom House 2013 (f) https://freedomhouse.org/report/freedom-press/2013/czech-republic

Freedom House 2013 (g), 'Indonesia' *Freedom House*, accessed at: https://freedomhouse.org/report/freedom-press/2013/indonesia#.VPHAGvTF_vA

Freedom House 2013, (h) 'Sri Lanka' *Freedom House*, accessed at: https://freedomhouse.org/report/freedom-net/2013/sri-lanka#.VPHMy_TF_vA

Freedom House. 2013 (i). Uzbekistan. Freedom House, accessed at: https://www.justice.gov/sites/default/files/eoir/legacy/2013/11/07/Uzbekistan_1.pdf

Freedom House 2012 (a) Freedom of the Press, Germany https://freedomhouse.org/report/freedom-press/2012/germany#.VGhxLYdhsj4

Freedom House 2012 (b) *Freedom on the Net*, China https://freedomhouse.org/report/freedom-net/2012/china#.VbC9_reAatw

Freedom House, 2011 (a) Germany, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2011/germany#.VGhsVldhsj4

Freedom House 2011 (b) 'License to Censor: The use of media regulation to restrict press freedom' - Uganda, 20 October, accessed 27 February 2015, accessed at: http://www.refworld.org/docid/4eccefc31c.html

Freedom House 2011c Freedom of the Press, El Salvador https://freedomhouse.org/report/freedom-press/2011/el-salvador#.VbDtobeAatw

Freedom House, 2010, Germany, Freedom of the Press, accessed at: https://freedomhouse.org/report/freedom-press/2010/germany#.VGhsEodhsj4

Folkbladet 2015 '*Anonymous sources may be revealed in the investigation*', Folkbladet, March 12: Accessed at < http://www.folkbladet.nu/1457948/anonyma-kallor-kan-rojas-i-utredningen >

Forcese C & Roach K, "How Ottawa's new terrorism act could chill free speech," *The Globe and Mail*, 5 February, accessed at: < http://www.theglobeandmail.com/globe-debate/how-ottawas-new-terrorism-act-could-chill-free-speech/article22799859/>

Fuchs C 2011, *WikiLeaks: power 2.0? Surveillance 2.0? Criticism 2.0? Alternative media 2.0? A political- economic analysis*, Global Media Journal - Australian Edition, 5:1. Available: http://www.hca.uws.edu.au/gmjau/archive/v5_2011_1/fuchs_RA.html

Gallagher, R, 2012, *Ecuador Implements "World's First" Countrywide Facial- and Voice-Recognition System*, Slate, December 12, accessed at: http://www.slate.com/blogs/future_tense/2012/12/12/surveillance_ecuador_implements_speech_technology_center_s_facial_and_voice.html

Gallagher R 2015, 'Researchers find 'astonishing' malware linked to NSA spying' *The Intercept*, 17 February, viewed 27 February 2015 at <https://firstlook.org/theintercept/2015/02/17/nsa-kaspersky-equation-group-malware/>

Garnica V 2014, 'Judge rules to move case against journalists in Bolivia to Press Tribunal', *International Press Institute*, 17 September, viewed 27 February 2015, accessed at: <http://www.freemedia.at/newssview/article/judge-rules-to-move-espionage-case-against-journalist-and-publisher-in-bolivia-to-print-tribun.html>

Garza Ramos, J (2015) Qualitative interview conducted by Jake Evans for UNESCO Internet Study: Privacy and Journalists' Sources

General Intelligence Laws Amendment Act 2013 (South Africa) accessed at: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf

Georgievski B 2015, "Macedonia reels over evidence of Orwellian surveillance," *Deutsche Welle*, 27 February, accessed at: < http://www.dw.com/en/macedonia-reels-over-evidence-of-orwellian-surveillance/a-18285626>

Giroux, H, 2015, *Totalitarian Paranoia in the Post-Orwellian Surveillance State*, Cultural Studies, 29:2, pp.108-140.

Global Journalist, 2012, *Legal victory for protection of sources, but press regulation still on the table*, May 15, accessed at: http://globaljournalist.org/2012/05/legal-victory-for-protection-of-sources-but-press-regulation-still-on-the-table

Gooch L 2011, 'Malaysian premier proposes replacing laws on detention' *The New York Times*, 16 September, accessed at: http://www.nytimes.com/2011/09/17/world/asia/malaysian-prime-minister-says-he-will-abolish-2-security-laws.html

Gold H 2015, 'Risen: Obama administration is greatest enemy of press freedom' *Politico*, 17 February, viewed 27 February 2015 at http://www.politico.com/blogs/media/2015/02/risen-obama-admin-is-greatest-enemy-of-press-freedom-202707.html

Greenberg A 2012, 'How to leak a secret in Bulgaria' *Slate*, 28 September, viewed 27 February 2015, accessed at: <http://www.slate.com/articles/technology/technology/2012/09/this_machine_kills_secrets_excerpt_how_balkanleaks_got_the_scoop_of_a_lifetime_.html>

Greenslade R 2015 'How can journalists protect their confidential sources from exposure?' *The Guardian*, 4 June. Accessed at: http://www.theguardian.com/media/greenslade/2015/jun/04/how-can-journalists-protect-their-confidential-sources-from-exposure

Greenslade R 2014, 'Plebgate fallout: police appear to have declared war on journalists,' *The Guardian*, 30 November, accessed at: http://www.theguardian.com/media/2014/nov/30/plebgate-police-war-on-journalists

Greenslade R 2009 Irish Times 'fined' for protecting sources', *The Guardian*. Accessed at: http://www.theguardian.com/media/greenslade/2009/nov/26/press-freedom-irish-times

Greenwald G 2014 *Tomgram: Glenn Greenwald, How I met Edward Snowden*, TomDispatch.com, May 13, accessed at: http://www.tomdispatch.com/post/175843/tomgram%3A_glenn_greenwald,_how_i_met_edward_snowden/

Greenwald G 2014b, 'On the UK's equating of Journalism with terrorism' *The Intercept*, 19 February, viewed 20 February, accessed at: https://firstlook.org/theintercept/2014/02/19/uks-equating-journalism-terrorism-designed-conceal-gchq/

Griffen S 2012, 'Press Freedom under Threat ahead of Dominican Republic Elections,' *International Press Institute*, 17 April, viewed 27 February, accessed http://www.freemedia.at/home/singleview/article/press-freedom-under-threat-ahead-of-dominican-republic-elections.html

Griffen, S, 2014, In Honduras, government secrecy law undermines promise of greater transparency, *International Press Institute*, January 20, accessed at: http://www.freemedia.at/newssview/article/in-honduras-government-secrecy-law-undermines-promise-of-greater-transparency.html

Guevara, M W, Ryle G, Olesen A, Cabra M, Hudson M, Giesen C 2014, 'Leaked records reveal offshore holdings of China's elite,' The International Consortium of Investigative Journalists, January 21, viewed 23 February 2015, http://www.icij.org/offshore/leaked-records-reveal-offshore-holdings-chinas-elite

Guja v. Moldova (Application no. 14277/04): Guja v. Moldova (Application no. 14277/04) 2008, *European Court of Human Rights*, 12 February, accessed at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-85016

Guyot, C (2015) Qualitative interview conducted by Alice Matthews for UNESCO Internet Study: Privacy and Journalists' Sources

Hakizimana 2014 *Bubanza : deux journalistes sommés de révéler leurs sources d'information*, IWACU http://www.iwacu-burundi.org/bubanza-deux-journalistes-sommes-de-reveler-leurs-sources-dinformation/

Hamrud, Annika "Source Protection in the center at the National Press Club""Källskyddet i centrum på Publicistklubben", Published 2007-10-15 23:15" http://www.dn.se/kultur-noje/kallskyddet-i-centrum-pa-publicistklubben/

Harding L 2013, "Footage released of Guardian editors destroying Snowden hard drives," *The Guardian*, 31 January, accessed at: <http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq>

Harlow, S, 2010, *New measures considered to protect journalists in Mexico*, Knight Centre, June 22, accessed at: https://knightcenter.utexas.edu/blog/new-measures-considered-protect-journalists-mexico

Hawley C 2009, "New Anti-Terror Legislation: Journalists Worry 'Big Brother Law' Will Kill Press Freedom," *Spiegel Online International*, 17 December, accessed at: http://www.spiegel.de/international/germany/new-anti-terror-legislation-journalists-worry-big-brother-law-will-kill-press-freedom-a-596807.html

Hellberg Magnus, 2015 'Murdered Elin's computer be seized despite criticism' *Expressen*, March 16, accessed at: < http://www.expressen.se/nyheter/mordade-elins-dator-tas-i-beslag-trots-kritik/>

Hendler, C, 2010, *A Swedish Shield, Unraised*, Columbia Journalism Review, September 2, accessed at: http://www.cjr.org/campaign_desk/a_swedish_shield_unraised.php?page=all

Hernandez MD 2014, 'Venezuela's new security agency: Watching the web with no judicial oversight' *Global Voices Online*, 19 March, viewed 27 February 2015, accessed at <http://advocacy.globalvoicesonline.org/2014/03/19/venezuelas-new-security-agency-watching-the-web-with-no-judicial-oversight/>

Heslop A 2014, 'UK Press Freedom Report' *WAN-IFRA*, 14 March, viewed 27 February 2015 at <http://www.wan-ifra.org/articles/2014/03/14/published-today-uk-press-freedom-report>

Hewitt D 2015, "China's New Draft Cybersecurity Law Increases Controls On Internet, Allows Officials To Switch Off Web Traffic During Public Protests," *International Business Times*, 8 July, accessed at: <http://www.ibtimes.com/chinas-new-draft-cybersecurity-law-increases-controls-internet-allows-officials-1999215>

Higuera, S, 2012, *Cybersecurity bill raises concerns among Panamanian journalists*, Knight Centre, October 2, accessed at: https://knightcenter.utexas.edu/blog/00-11592-cybersecurity-bill-raises-concerns-among-panamanian-journalists

Higuera, S, 2013, *Peruvian Attorney General asks journalist to reveal his sources*, Knight Centre, March 4, accessed at: https://knightcenter.utexas.edu/blog/00-13122-peruvian-attorney-general-asks-journalist-reveal-his-sources

Higuera, S 2015 Qualitative interview conducted by Alice Matthews for UNESCO Internet Study: Privacy and Journalists' Sources

Hillebrand, Claudia, 2012, "The Role of News Media in Intelligence Oversight," *Intelligence and National Security*, 27:5, 689-706

Hirsch, A, 2010, *Iceland aims to become a legal safe haven for journalists*, The Guardian, July 12, accessed at: http://www.theguardian.com/media/2010/jul/12/iceland-legal-haven-journalists-immi

Hobday L 2011, 'Police Raid Melbourne Age Office' *The World Today*, 15 December, accessed at: http://www.abc.net.au/worldtoday/content/2011/s3391414.htm

Högsta Domstolen 2015, *Högsta domstolen häver beslag av fotografier av ett skyddsobjekt med hänvisning till yttrandefrihetsgrundlagarnas anskaffarfrihet, The Supreme Court*, Sweden, June 5, accessed at: http://www.hogstadomstolen.se/Mer-om-Hogsta-domstolen/Nyheter-fran-Hogsta-domstolen/Hogsta-domstolen-haver-beslag-av-fotografier-av-ett-skyddsobjekt-med-hanvisning-till-yttrandefrihetsgrundlagarnas-anskaffarfrihet/

Holcomb J, Mitchell A & Page D 2015 'Investigative Journalists and Digital Security': *Perceptions of Vulnerability and Changes in Behaviour*, 5 February. Accessed at: http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/

Holmes T 2013, 'ConCourt rejects Bosasa's appeal to expose M&G sources,' *Mail & Guardian*, 1 February, accessed at: http://mg.co.za/article/2013-01-31-concourt-rejects-bosasas-appeal-to-expose-mg-sources

Hong Chieh Y 2010, "The Star challenges SC's powers in court," *The Malaysian Insider*, 1 July, accessed at: http://www.themalaysianinsider.com/malaysia/article/the-star-challenges-scs-powers-in-court#sthash.OlR9jPLk.dpbs

Hong Kong Journalists' Association 2013, accessed at: < http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-1088&lang=zh-TW>, cited in InMedia Hong Kong 2015 http://www.inmediahk.net/node/1033428

Horsley W 2012, "OSCE Safety of journalists guidebook," *Office of the OSCE Representative on Freedom of the Media*, accessed at: https://www.osce.org/fom/85777?download=true

Horwitz S 2013, "Julian Assange unlikely to face U.S. charges over publishing classified documents," *The Washington Post*, 25 November, accessed at: https://www.washingtonpost.com/world/national-security/julian-assange-unlikely-to-face-us-charges-over-publishing-classified-documents/2013/11/25/dd27decc-55f1-11e3-8304-caf30787c0a9_story.html

Hughes, Sunny Skye, 2012, 'US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program,' *Canadian journal of law and society*, 27:3, pp 399-425

Human Rights Watch (HRW) 2015a, 'Burundi: Prominent radio journalist arrested', *Human Rights Watch*, 22 January, accessed at: http://www.hrw.org/news/2015/01/22/burundi-prominent-radio-journalist-arrested

Human Rights Watch (HRW) 2015b *Pakistan's New Cybercrime Bill Threatens Rights* http://www.hrw.org/news/2015/04/20/pakistan-cybercrime-bill-threatens-rights

Human Rights Watch (HRW) 2014a *Liberty to Monitor All* https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

Human Rights Watch (HRW) 2013b, 'Uganda: Stop Harassing the Media', *Human Rights Watch*, May 20, accessed at: http://www.hrw.org/news/2013/05/20/uganda-stop-harassing-media_

Human Rights Watch (HRW) 2013a *India's New Monitoring System Threatens Rights* http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights

Hurst D 2015, "Australia's new 'improved' data retention laws: how will they work?," *The Guardian*, 19 March, accessed at: < http://www.theguardian.com/media/2015/mar/19/australias-new-improved-data-retention-laws-how-will-they-work>

Husovec M, Lukic L 2014, 'The quest for privacy in Slovakia: The case of data retention' *European Information Society Institute*, viewed 27 February 2015 at: <http://www.giswatch.org/en/country-report/communications-surveillance/slovak-republic>

Hurst D 2015, 'Senators and MPs back data retention scheme but want more safeguards', *The Guardian*, 27 February, accessed at: http://www.theguardian.com/australia-news/2015/feb/27/senators-and-mps-back-data-retention-scheme-but-want-more-safeguards

Husovec & Lukic 2014, "The quest for privacy in Slovakia: The case of data retention," *GIS Watch*, accessed at: <http://www.giswatch.org/en/country-report/communications-surveillance/slovak-republic>

IAPA, 2014, Uruguay, 2014- Midyear Meeting – Bridgetown, Inter American Press Association, accessed at: http://www.sipiapa.org/en/asamblea/uruguay-87

IAPA, 2013, Panama, 2013 – General Assembly of the IAPA – Denver, Estados Unidos, accessed at: http://www.sipiapa.org/en/asamblea/panama-133/

IAPA, 2009, Argentina, General Assembly Buenos Aires, Inter American Press Association, accessed at: http://www.sipiapa.org/en/asamblea/argentina-35/

ICIJ 2015, 'Secrecy for Sale: Inside the global offshore money maze', *The International Consortium of Investigative Journalists*, viewed 20 February 2015, http://www.icij.org/offshore

ICIJ 2015, 'Luxembourg Leaks: Global Companies' Secrets Exposed', *The International Consortium of Investigative Journalists*, viewed 23 February 2015, http://www.icij.org/project/luxembourg-leaks

ICIJ 2015, 'Swiss leaks: murky cash sheltered by bank secrecy' *International Consortium of Investigative Journalists*, viewed 27 February 2015, accessed at: http://www.icij.org/project/swiss-leaks

ICJ 2012 International Commission of Jurists, 'Submission to the Universal periodic review of Indonesia' *United Nations Human Rights Council 13 session of the working group on the Universal Periodic Review*, 11 November, accessed at: http://www.icj.org/wp-content/uploads/2012/05/Indonesia-ICJ-submission-UPR-legal-submission-2011.pdf

IFEX 2010, "Thirty-one IFEX members and global partners demand retraction of proposed amendment to Press and Journalists Act," *Freedom House*, 7 September, accessed at: http://www.ifex.org/uganda/2010/09/07/press_journalist_act/

IFEX 2015, 'Mass surveillance endangers freedom of expression in Macedonia,' *IFEX*, 11 February, viewed 27 February 2015, accessed at: https://www.ifex.org/macedonia/2015/02/11/mass_surveillance/?i=1

Information and Communications Act 2009, Gambia, entered into force May 2009, made available online by the *World Intellectual Property Organisation (WIPO)*, accessed at: http://www.wipo.int/edocs/lexdocs/laws/en/gm/gm006en.pdf

India, 2008. Information Technology (Amendment) Act, 2008, India, published in the Gaxette of India Part II, Section 1, Ministry of Law and Justice (Legislative department) New Delhi, February 5 2009, accessed at: http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

Institute for Development of Freedom of Information 2014, 'Internet Freedom in Georgia – Report N3 – 4' *IDFI* 16 September, viewed 27 February 2015, at < https://idfi.ge/en/internet-freedom-in-georgia-report-n3-4>

Inter American Press Association 2013, 'Panama', *Assembly: 2013, General Assembly of the IAPA – Denver, Estados Unidos, Reports*, viewed 27 February, accessed at: <http://www.sipiapa.org/en/asamblea/panama-133/>

Inter American Press Association 2014, 'Uruguay', *Assembly: 2014 – Midyear Meeting, Bridgetown, Barbados,* viewed 27 February 2015, accessed at http://www.sipiapa.org/en/asamblea/uruguay-87/

Interception of Communications Commissioner's Office 2015, 'IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources' *IOCCO*, 4 February, accessed 27 February 2015 at: http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

IPI 2014a *Costa Rica Court Surveillance of Journalists Was Unconstitutional* http://www.freemedia.at/newssview/article/costa-rica-court-surveillance-of-journalist-was-unconstitutional.html

IPI 2014b *Costa Rican Reporter Endures Months of Police Monitoring* http://www.freemedia.at/newssview/article/costa-rican-reporter-endures-months-of-police-monitoring.html

IPI 2014c, 'New telecommunications law in Mexico endangers both journalists and their sources, experts say' *International Press Institute*, 17 September, viewed 27 February 2015 at < http://www.ipinewsinnovation.org/news/telecommunications-law-mexico.html>

IPI via IFEX, 2013, *Nigerian journalists detained for refusing to disclose source*, via International Press Institute, April 9, accessed at: https://www.ifex.org/nigeria/2013/04/09/source_protection

InMedia 2015, "Hong Kong In-Media Statement: Interception of Communications and Surveillance Ordinance Outdated, requires drastic amendment to prevent political surveillance," *InMedia Hong Kong*, 16 April, accessed at: http://www.inmediahk.net/node/1033428

Instituto Prensa y Sociedad and IFEX (IPYS/IFEX) 2012, 'Peru blocks access to national security information', IFEX, December 12, accessed at: https://www.ifex.org/peru/2012/12/12/decreto_defensa/

International Law Office, 2014b, *Media & Entertainment - Switzerland, Denial of protection of journalist's source*, http://www.internationallawoffice.com/newsletters/Detail.aspx?g=91419c11-814f-499d-94d0-127f030ecf1f

International Modern Media Institute, 2014, *Icelandic Modern Media Initiative: progress report*, accessed at: https://en.immi.is/immi-resolution/progression/

IREX, 2014, Media Sustainability Index 2014 – Former Yugoslavian Republic of Macedonia, accessed at: http://www.irex.org/sites/default/files/u105/EE_MSI_2014_Macedonia.pdf

IREX 2012 Media Sustainability Index 2012, Sudan https://www.irex.org/sites/default/files/u115/Sudan.pdf

IRIS, 2012. *IRIS Merlin*, accessed at: http://merlin.obs.coe.int/iris/2012/7/article14.en.html

ISCP 2015, "Privacy and Security: A modern and transparent legal framework," *Intelligence and Security Committee of Parliament, Crown*, 12 March, accessed at: <https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cpAan4WecKUl4V7wPXYnwXSl2nczwwEA9_dINb-K2j_uuAHRdB7OH0KjG07l9BReteEvkEzwJWEdpfOWMU-tDcoD4mYs01Fcdq6ofVn5ghkJEtjQcu2VmnI11do5tz8mK1kwD9_yTwGKKJBrimbcDmbFP3IluneoHBl24B9V-VYTrXy_dhkHAqvicYIPl4pha7Xad2iVknx3kx_w57mM2KaeEnG6-NGYNmrKAm-hTqoVwJlvk36wvbp3jEVSdFE9OIMCmb8&attredirects=0>

ISO/IEC FDIS 11179-1 2004 "Information technology - Metadata registries - Part 1: Framework", March, accessed at: < http://stats.oecd.org/glossary/detail.asp?ID=4575>

IWACU 2014 Bubanza : deux journalistes sommés de révéler leurs sources d'information http://www.iwacu-burundi.org/bubanza-deux-journalistes-sommes-de-reveler-leurs-sources-dinformation/

Jakarta Post 2012, 'Court rejects request for Intelligence law review' *The Jakarta Post*, 11 October, accessed at http://www.thejakartapost.com/news/2012/10/11/court-rejects-request-intelligence-law-review.html

Jedou, A, 2014, '*Activists Push Back on Mauritania's Information Society Law*', Global Voices Advocacy, May 12, accessed at: http://advocacy.globalvoicesonline.org/2014/05/13/activists-push-back-on-mauritanias-information-society-law/

Jordan W 2015, 'Spy cables raise South Africa privacy concerns' *Al Jazeera*, 25 February, accessed at: http://www.aljazeera.com/news/2015/02/spy-cables-raise-south-africa-privacy-concerns-snowden-surveillance-guardian-150225161131481.html

Journalism.co.za 2011, ' Media regulation in Lesotho in limbo' *Journalism.co.za*, 3 February, accessed at: http://www.journalism.co.za/blog/media-regulatotion-in-lesotho-in-limbo/

Journalist's Statute Law no. 01/99 (Portugal), accessed at: http://www.gmcs.pt/en/journalists-statute

Kaye D 2015, "Report on encryption, anonymity, and the human rights framework," *Office of the High Commissioner for Human Rights*, accessed at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Keita M 2011, 'Attacks on the Press 2010:Africa Analysis - Across continent, governments criminalize investigative reporting,' *Committee to Protect Journalists*, 15 February, accessed at: https://www.cpj.org/2011/02/attacks-on-the-press-2010-africa-analysis.php)

The Kenya Information and Communications (amendment) Act (No. 41.A of 2013): The Kenya Information and Communications (amendment) Act (No. 41.A of 2013) accessed at: http://www.mediacouncil.or.ke/en/mck/jdownloads/Media%20Laws/the_kenya_information_and_communications_amendment_act_2013.pdf

Kenya's Media Council Act 2013, accessed at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/MediaCouncilAct2013.pdf

Khan, A 2013, *New computer crimes law in Peru threatens freedom of information, organizations say*, October 31, accessed at: https://knightcenter.utexas.edu/blog/00-14689-new-computer-crimes-law-peru-threatens-freedom-information-organizations-say

Khoza M 2015, 'Mpumalanga Premier said to be getting spy reports on journalists,' *The Sunday Independent*, 10 February, accessed at: http://www.iol.co.za/sundayindependent/mpumalanga-premier-said-to-be-getting-spy-reports-on-journalists-1.1815999#.VNoZ2cbnteZ

Kravets D 2015, 'Gag order prevented Google from disclosing WikiLeaks probe for 3 years' *Ars Technica*, 28 January, viewed 27 February 2015: < http://arstechnica.com/tech-policy/2015/01/gag-order-prevented-google-from-disclosing-wikileaks-probe-for-3-years/>

Kubacki K 2014, 'Uganda circulates draft data protection and privacy bill 2014 for public consultation' *First Advantage*, 4 December, viewed 27 February 2015, accessed at: http://www.fadv.com/company/blog/entry/articletype/articleview/articleid/152/uganda-circulates-draft-data-protection-and-privacy-bill-2014-for-public-consultation.aspx

Kugathasan A 2013, 'War on terrorism versus civil liberties of individuals: An analysis of the Malaysian Security Offences (Special Measures) Act 2012' *University for Peace: Peace & Conflict Monitor*' 2 November, accessed at: http://www.monitor.upeace.org/archive.cfm?id_article=961

Kuttab, D (2015) Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

La Lay 17.671 SIBIOS (Argentina), accessed at: http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

La Rue, F, 2013, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, accessed at: http://daccess-ddsny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement accessed 23.11.14

La Verdad 2012, 'CNP Zulia defiende a La Verdad y su derecho a proteger la fuente' *La Verdad*, viewed 27 February 2015, accessed at: <http://www.laverdad.com/sucesos/20419-cnp-zulia-defiende-a-la-verdad-y-su-derecho-al-secreto-de-la-fuente.html>

Laville, Sandra, 2013, 'Operation Elveden expansion to include unpaid leakers provokes alarm,' *The Guardian*, 22 March, Available: http://www.theguardian.com/uk/2013/mar/21/operation-elveden-expansion-unpaid-leaks

Lara, T 2013a, *Guatemalan prosecutors ask reporter to reveal source of leaked prison report*, March 25, accessed at: https://knightcenter.utexas.edu/blog/00-13311-guatemalan-prosecutors-ask-reporter-reveal-source-leaked-prison-report

Lara T 2013b, 'Security agency accuses journalist in Venezuela of inciting crime through his reporting Knight Centre for Journalism in the Americas' *Journalism in the Americas, The University of Texas at Austin*, 6 February, viewed 27 February 2015, accessed at https://knightcenter.utexas.edu/blog/00-12837-security-agency-accuses-journalist-venezuela-inciting-crime-through-his-reporting

Lara, T 2012a, *Journalist denounces persecution after revealing that Dominican Republic senator donated to Haitian presidential campaign*, Knight Centre, April 5, accessed at: https://knightcenter.utexas.edu/blog/00-9654-journalist-denounces-persecution-after-revealing-dominican-republic-senator-donated-hai

Lara, T 2012b, *Mexican newspaper journalist held at mayor's office, forced to reveal source*, Knight Centre, March 15, accessed at: https://knightcenter.utexas.edu/blog/00-9326-mexican-newspaper-journalist-held-mayors-office-forced-reveal-source

Lara T 2012c 'Proposed law would fine, jail Dominican journalists without university degree' *Journalism in the Americas, The University of Texas Austin*, 23 February, viewed 27 February 2015, accessed at < https://knightcenter.utexas.edu/blog/00-9137-proposed-law-would-fine-jail-dominican-journalists-without-university-degree>

Lara T 2011 *Ex-mayor in Honduras receives death threats after being accused of acting as anonymous source for drug trafficking story*, Knight Centre, August 29, accessed at: https://knightcenter.utexas.edu/blog/ex-mayor-honduras-receives-death-threats-after-being-accused-acting-anonymous-source-drug-traff

Latin American Herald Tribune 2015 *Colombian Ex-Spy Chief Gets 14-Year Sentence* http://www.laht.com/article.asp?ArticleId=2385815&CategoryId=12393).

Lauría C 2010 *In the Americas, Big Brother is watching reporters*, Committee to Protect Journalists, February 16, accessed at: https://cpj.org/2010/02/in-the-americas-big-brother.php

Laurin, F (2014/2015) Qualitative interviews conducted by Federica Cherubini and Angelique Lu/Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

Law No. 12.965 Presidency of the Republic, Civil House, Subchefia for Legal Affairs, of 23 April 2014, (Brasil), accessed at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Learner, Jack and Bar-Nissim, Rom, 2014, "Law Enforcement Investigations Involving Journalists," Legal Studies Research Paper Series No. 2014-71, School of Law, University of California, Irving.

Legal framework of the Mauritanian Information Society, 2014: accessed at http://www.emploi.gov.mr/NR/rdonlyres/1C0A8D57-B8F5-4E05-BEEE-07C5194AB1D2/0/ProjetduCadreJuridiqueSeptembre2014FR.pdf

Legal Information Institute, date unknown, '42 U.S. Code § 2000aa - Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses,' *Cornell University Law School*, accessed at: https://www.law.cornell.edu/uscode/text/42/2000aa

Legislative Decree 108 for 2011, (Syria) accessed at: http://www.syriaonline.sy/details.php?t=syria&id=1845

Leslie G 2008 'What's up with Wyoming and the reporter's privilege?' Reporters Committee for Freedom of the Press, accessed at: http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-fall-2008/whats-wyoming-and-reporters-p#sthash.RL2mn8Z7.dpufLeveson B 2012 *Leveson Inquiry Final Report* http://webarchive.nationalarchives.gov.uk/20140122145147/http:/www.levesoninquiry.org.uk/about/the-report/

Lewis J A 2014, 'Reference Note on Russian Communications Surveillance', *Center for Strategic & International Studies (CSIS),* April 18, accessed at: http://csis.org/publication/reference-note-russian-communications-surveillance

Ley de Telecomunicaciones y Radiodifusión 2014 http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014)

Ley 20453 2010 http://www.leychile.cl/Navegar?idLey=20453)

Lidberg J 2013, 'Pennells decision a win for source protection and investigative journalism,' *The Conversation*, 8 August, accessed at: https://theconversation.com/pennells-decision-a-win-for-source-protection-and-investigative-journalism-16755

Limpitlaw J 2013 *Media Law Handbook for Southern Africa*, vol 2, KAS, South Africa, pp 476-477, accessed at: http://www.kas.de/wf/doc/10507-1442-2-30.pdf

Limpitlaw J 2014 Qualitative interview conducted by Angelique Lu for UNESCO Internet Study: Privacy and Journalists' Sources

Loh D 2010 *The Securities Commission's Power*, The Nut Graph, 13 July, accessed at: http://www.thenutgraph.com/the-securities-commission%E2%80%99s-powers/

Loi renseignement 2015 http://www.senat.fr/leg/pjl14-424.html

Lomas N 2015, "U.K. Government Confirms Push For More Comms Data Capture Powers," *Tech Crunch*, 27 May, accessed at: http://techcrunch.com/2015/05/27/u-k-government-confirms-push-for-more-comms-data-capture-powers/#.bfjbtu:0FX1

Ludlow P 2013, 'The Strange case of Barrett Brown' *The Nation*, 18 June, accessed at: <http://www.thenation.com/article/strange-case-barrett-brown/>

Maass P 2015, 'Destroyed by the espionage act' *The Intercept*, 18 February, viewed 27 February 2015 at: < https://firstlook.org/theintercept/2015/02/18/destroyed-by-the-espionage-act/>

Macau, China: National Security Law, 2/2009

Mageswari, M, 2014, *Reporter need not reveal source*, The Star Online, 30 August, accessed at: http://www.thestar.com.my/News/Nation/2014/08/30/Reporter-need-not-reveal-source-Tiongs-appeal-incompetent-says-court/

Mahon Tribunal v Keena & anor [2009] IESC 78 accessed at: <http://www.supreme-court.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/8943753bff3d-97b28025767a003d3d1f?OpenDocument>

Mail & Guardian 2010, 'Subpoena against e.tv "infringes media freedom,"' 21 January, accessed at: http://mg.co.za/article/2010-01-21-subpoena-against-etv-infringes-media-freedom

Mail & Guardian 2014, 'Outrage over sedition charge agaisnt Botswana journalist', *Mail & Guardian*, September 11, accessed at: http://mg.co.za/article/2014-09-11-outrage-over-sedition-charge-agaisnt-botswana-journalist/

Majumdar A 2013, *UK government raids Guardian's offices, wants to nip Snowden stories in the bud*, Tech First Post, August 20, accessed at: http://tech.firstpost.com/news-analysis/uk-government-raids-guardians-offices-wants-to-nip-snowden-stories-in-the-bud-104203.html

Maina H 2015 Qualitative interview conducted by Alexandra Waldhorn for UNESCO Internet Study: Privacy and Journalists' Sources

Mahon Tribunal v Keena & anor [2009] IESC 78 accessed at: <http://www.supreme-court.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/8943753bff3d-97b28025767a003d3d1f?OpenDocument>

Malumo R 2010 'South Africa: e.tv journalists appears in court for concealing sources,' *Friedrich Ebert Stiftung Media*, 25 January, accessed at: <http://www.fesmedia-africa.org/what-is-news/statements-developments/news/article/south-africa-etv-journalists-appears-in-court-for-concealing-sources/>

Manhire T 2015 New Zealand spying on Pacific allies for 5 Eyes and NSA Snowden files show http://www.theguardian.com/us-news/2015/mar/05/new-zealand-spying-on-pacific-allies-for-five-eyes-and-nsa-snowden-files-show

Marquis-Boire M, Marczak B, Guarnieri C, Scott-Railton J 2013, 'You only click twice: FinFisher's Global Proliferation,' *Citizen Lab*, March, accessed at: https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Martínez, A, 2013, *Ecuador's controversial Communications Law in 8 points*, Knight Centre, June 20, accessed at: https://knightcenter.utexas.edu/blog/00-14071-8-highlights-understand-ecuador%E2%80%99s-controversial-communications-law

Mason R 2015, 'Culture secretary Sajid Javid: journalism is not terrorism' *The Guardian*, 5 February, viewed 27 February 2015 at: <http://www.theguardian.com/world/2015/feb/05/culture-secretary-sajid-javid-journalism-not-terrorism>

Marczak B, Scott-Railton J, & McKune S 2015, "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware," *Citizen Lab*, 9 March, accessed at: https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/

Marimow A 2013, 'A rare peek into a Justice Department leak probe,' *The Washington Post*, 19 May, accessed at: < http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html>

May A 2015, 'Report of the Interception of Communications Commissioner,' *Crown*, March, accessed at: http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf

Mayr W 2011, 'The Goulash Archipelago: EU remains silent as Hungary veers off course' *Spiegel Online International* 19 August, viewed 27 February 2015, accessed at: http://www.spiegel.de/international/europe/the-goulash-archipelago-eu-remains-silent-as-hungary-veers-off-course-a-780794-2.html

Mazotte 2012, *Uruguayan journalist says his cell phone was intercepted after reporting on military*, Knight Centre, April 4, accessed at: https://knightcenter.utexas.edu/blog/00-9611-uruguayan-journalist-says-his-cell-phone-was-intercepted-after-reporting-military

McCracken P n.d., 'Kyrgyzstan' *International Press Institute*, accessed at: http://www.freemedia.at/newssview/article/kyrgyzstan.html

McGauran K 2009 'Germany Permanent state of pre-emption,' *State Watch*, accessed at: http://www.statewatch.org/analyses/no-79-germany-permanent-state-of-preemption.pdf

McKinnon R, Hickok E, Bar A, Lim H 2014 *Fostering Freedom Online: The Role Of Internet Intermediaries*. Unesco/Internet Society 2014. Print. Unesco Series On Internet Freedom, accessed at: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

McGregor, S 2015 Qualitative interview conducted by Angelique Lu for UNESCO Internet Study: Privacy and Journalists' Sources

Meade, A 2015 'Data Retention Bill Far Too Intrusive Says New Press Council Chair' in *The Guardian* 9/03/15 <http://www.theguardian.com/technology/2015/mar/09/data-retention-bill-far-too-intrusive-says-new-press-council-chair-david-weisbrot?CMP=soc_567

Medel M 2011 *State legislature passes first law in Mexico protecting secrecy of journalists' sources*, Knight Centre, June 29, accessed at: https://knightcenter.utexas.edu/blog/state-legislature-passes-first-law-mexico-protecting-secrecy-journalists-sources

Medel 2011 b *Peru's Congress Secretly Investigated Phone Calls* https://knightcenter.utexas.edu/blog/perus-congress-secretly-investigated-phone-calls-journalists-who-alleged-corruption

Media.Am 2014 http://media.am/en/armenian-journalist-info-source-case-in-court

Media, Entertainment & Arts Alliance 2015 'MEAA condemns Data Retention Bill's hunt for journalists' sources' *Media, Entertainment & Arts Alliance*, 27 February, accessed at: http://www.alliance.org.au/meaa-condemns-data-retention-bills-hunt-for-journalists-sources

Mendel, T 2015 Qualitative interview conducted by Marcus O'Donnell for UNESCO Internet Study: Privacy and Journalists' Sources

Millar, G 2015 Qualitative interview conducted by Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

Ministère de la Justice 2013, 'Protection du secret des sources des journalistes,' 12 June, viewed 27 February 2015 at < http://www.justice.gouv.fr/la-garde-des-sceaux-10016/protection-du-secret-des-sources-des-journalistes-25622.html

Ministry of Communications Cote d'Ivorie, 2012, acccessed at: http://www.communication.gouv.ci/?code=code

Mir W, Ali W, Niazi H Tariq K, n.d., 'Digital Surveillance Laws in Pakistan: A white paper by Digital Rights Foundation', accessed at: http://jasoosibandkaro.pk/whitepaper/

Moore, Martin, 2014, "RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework," *The Political Quarterly*, 85:2, 125-132

Mueller C, Narim K 2014, 'Controversial cybercrime law 'scrapped," *Cambodia Daily*, 12 December, accessed at: https://www.cambodiadaily.com/news/controversial-cybercrime-law-scrapped-74057/;

Musisi F 2014, 'Cabinet approves Bill to protect phone records' *Daily Monitor*, 24 January, viewed 27 February 2015, accessed at http://www.monitor.co.ug/News/National/Cabinet-approves-Bill-to-protect-phone-records/-/688334/2158008/-/159t075z/-/index.html

National Council of the Slovak Republic, 2011, *Amendment Act no. 221/2011 of the Press Act*, www.culture.gov.sk/legdoc/56/

National Legislative Bodies / National Authorities 2009, *Ethiopia: Proclamation No. 652/2009 of 2009, Anti-Terrorism Proclamation*, 7 July 2009, accessed at: http://www.refworld.org/docid/4ba799d32.html National Security Legislation Amendment Bill [No. 1 2014] (Cth), viewed 20 July 2015, accessed at: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s969

Nelson K 2014 *Apple Pulls Secret App in Brazil after Judge's Request*, Mashable, August 23, accessed at: http://mashable.com/2014/08/22/secret-app-brazil/

Neuberger D 2014 'The Third and Fourth Estates: Judges, Journalists and Open Justice', presented at the Hong Kong Foreign Correspondents' Club, 26 August. Accessed at: https://www.supremecourt.uk/docs/speech-140826.pdf

Newman M 2015 'Boost for press freedom campaign as European court prioritises Bureau's legal challenge to UK snooping laws,' *The Bureau Investigates*, 20 January, accessed at: https://www.thebureauinvestigates.com/2015/01/20/boost-press-freedom-european-court-bureau-case-snooping-laws/

Newman M 2015 'Former GCHQ legal director: Journalists' communications not considered in RIPA drafting,' *The Bureau of Investigative Journalism*, 9 February, viewed 27 February 2015 at: http://www.thebureauinvestigates.com/2015/02/09/former-gchq-legal-director-journalists-communications-not-considered-in-ripa-drafting/

New Zimbabwe 2013, 'Call to align media laws with Constitution', New Zimbabwe, November 23, accessed at: http://www.newzimbabwe.com/news-13212-Call+to+align+media+laws+with+Constitution/news.aspx

Nforngwa E 2014 'Peter Essoka takes distance from military court,' *The Standard-Tribune*, 3 November, accessed at: http://www.standard-tribune.com/?p=1985

NITA 2014, 'Request for Comments on the Draft Data Protection and Privacy Bill, 2014', National Information Technology Authority - Uganda (NITAU), November 15, accessed at: http://www.nita.go.ug/media/request-comments-draft-data-protection-and-privacy-bill-2014 NJCM 2015, 'European Court of Human Rights: Seizure of Dutch journalist's confidential photographs illegal' Nederlands Juristen Comité voor de Mensenrechten, 15 December, accessed at: http://www.njcm.nl/site/jurisprudentie/show/58>

Nolan D 2015, 'Europe's Journalists Caught in Widening National Security Net,' *Center for Media, Data and Society CEU School of Public Policy*, February 13, accessed at: http://journalism.cmpf.eui.eu/discussions/europes-journalists-caught-in-widening-national-security-net/

Noorlander P 2014 'Finding Justice for Whistleblowers,' *Center for Media, Data and Society*, CEU School of Public Policy, 5 December, accessed at: http://journalism.cmpf.eui.eu/discussions/finding-justice-for-whistleblowers/

Noorlander, P 2015 Qualitative interview conducted by Emma Goodman for UNESCO Internet Study: Privacy and Journalists' Sources

Noticeros Televisa 2014 *Nuevas disposiciones a la ley del secreto profesional del periodista* http://noticieros.televisa.com/mexico-df/1409/nuevas-disposiciones-ley-secreto-profesional-periodista/

NUSOJ 2014 *Somali government passes anti-media legislation*, National Union of Somali Journalists, September 2, accessed at: http://www.nusoj.org/2014/09/02/somali-government-passes-anti-media-legislation/

NUJ 2014 *Source Protection Law Now Submitted to Dutch Lower House* https://nuj-netherlands.nl/12-public/news-summaries/96-source-protection-law-now-submitted-to-dutch-lower-house

Nygren G 2015 Qualitative interview conducted by Angelique Lu for UNESCO Internet Study: Privacy and Journalists' Sources

O'Carroll L 2015, 'Met police to face tribunal over decision to access Plebgate phone records,' *The Guardian* 14 July, accessed at: < http://www.theguardian.com/uk-news/2015/jul/14/met-police-investigatory-powers-tribunal-plebgate-sun-phone-records>

O'Carroll L 2014, 'Sun makes official complaint over police use of Ripa against journalists', *The Guardian*, 6 October, accessed at: < http://www.theguardian.com/media/2014/oct/06/sun-official-complaint-ripa-journalists-met-police>

O'Carroll Lisa 2012 'The Sun's Trevor Kavanagh: News Corp team 'boasting' over help to police', *The Guardian*, 14 February, Available: http://www.theguardian.com/media/2012/feb/13/sun-trevor-kavanagh-news-corp

Odera A, 2014, Survey response to *Protecting Journalists' Sources in the Digital Era*

O'Donnell, L 2015 Qualitative interview conducted by Marcus O'Donnell for UNESCO Internet Study: Privacy and Journalists' Sources

OECD 2013, 'CleanGovBiz Integrity in Practice, Investigative Media,' Secretary General of the OECD, accessed at: http://www.oecd.org/cleangovbiz/InvestigativeMediaDraft.pdf

Office of the Cabinet of Ministers Sri Lanka 2012, 'Press Briefing of cabinet decision taken on 2012-07-11' *Office of the Cabinet of Ministers Sri Lanka*, http://www.cabinetoffice.gov.lk/cab/index.php?option=com_content&view=article&id=16&Itemid=49&lang=en&dID=4617

Ogunseye T 2015 Qualitative interview conducted by Federica Cherubini for UNESCO Internet

OHCHR (UN) 2012a, "*ASEAN Human Rights Declaration should maintain international standards*," *urge key UN expert group*, November 2012, accessed at http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=12796&LangID=E ;

OHCHR (UN) 2012b, *Pillay encourages ASEAN to ensure Human Rights Declaration is implemented in accordance with international obligations*, November 19, accessed at http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=12809&LangID=E

OHCHR (UN) 2014, *The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights*, June 30, accessed at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Oldroyd R 2014, Bureau files ECHR case challenging UK government over surveillance of journalists' communications, *The Bureau of Investigative Journalism*, September 14, accessed at: http://www.thebureauinvestigates.com/2014/09/14/bureau-files-echr-case-challenging-uk-government-over-surveillance-of-journalists-communications/

Omanovic E 2014, 'Private Interests: Monitoring Central Asia', *Privacy International*, 20 November, accessed at: https://www.privacyinternational.org/?q=node/59

OpenNet Africa, n.d. Burundi. Accessed at: http://opennetafrica.org/country-profiles/burundi/

OpenNet Africa 2013 'Uganda's assurances on social media monitoring ring hollow' June 10, viewed 24 February 2015. Accessed at: http://opennetafrica.org/ugandas-assurances-on-social-media-monitoring-ring-hollow/

OpenNet Africa 2015, 'Reflections on Uganda's Draft Data Protection and Privacy Bill, 2014', 26 February, accessed at: http://www.opennetafrica.org/uganda-data-protection-privacy-bill/

Open Society Foundations 2014a, 'Japan's State Secrecy law faulted in human rights review', *Open Society Foundations*, 13 August, accessed at: http://www.opensocietyfoundations.org/voices/japans-state-secrecy-law-faulted-human-rights-review

Open Society Foundations 2014b, 'Case Watch: Peru's Constitutional Court Hears Challenge to Blanket Military Secrecy' 30 October, viewed 27 February 2015 http://www.opensocietyfoundations.org/voices/case-watch-perus-constitutional-court-hears-challenge-blanket-military-secrecy

Open Society Foundations (OSF) 2014c, 'Executive Decree 1129', *Open Society Foundations*, March 14, accessed at: https://www.opensocietyfoundations.org/litigation/executive-decree-1129

Ordinance No. 2010-035 (Niger), accessed at: http://www.medianiger.info/Index.asp?affiche=News_Display.asp&articleid=1982&ID=88&SID=17

Organic Communication Law 2013 (Ecuador), accessed at: http://fr.slideshare.net/paularomo/proyecto-de-ley-de-comunicacin-04042012

Organic Penal Code Ecuador 2013 (Ecuador), accessed at: http://www.lahora.com.ec/frontEnd/images/objetos/C%C3%B3digo_Penal.pdf

Organization of American States 2011, 'Mandatory membership in a professional association for the practise of journalism,' *Organization of American States*, viewed 27 February 2015, accessed at < http://www.oas.org/en/iachr/expression/showarticle.asp?artID=154&lID=1>

OSCE 2015, 'French draft law on surveillance threat to journalists' right to protection of sources, says OSCE Representative" *OSCE*, 6 May, accessed at: <http://www.osce.org/fom/155336>

http://www.osce.org/fom/129941

OSCE 2014b 'Switzerland should safeguard journalists' right to protection of sources', *Organization for Security and Co-operation in Europe*. Accessed at: http://www.osce.org/fom/115553

OSCE, 2014c, 'OSCE Representative welcomes court decision declaring wiretapping of journalists in Lithuania illegal', *Organization for Security and Co-operation in Europe*, August 29. Accessed at: http://www.osce.org/fom/123032

OSCE 2014d, 'OSCE media freedom representative concerned by attempts to force Polish journalists to reveal sources,' *Organization for Security and Co-operation in Europe*, 19 June. Accessed at: http://www.osce.org/fom/120003

OSCE 2013, 'OSCE media freedom representative deeply concerned over today's conviction of journalist in Skopje,' *Organization for Security and Co-operation in Europe*, 21 October. Accessed at: <http://www.osce.org/fom/107265>

OSCE 2011, 'Vilnius Recommendations on Safety of Journalists', *Organization for Security and Co-operation in Europe*, 8 June. Accessed at: http://www.osce.org/cio/78522

OSCE 2008, 'OSCE media freedom representative urges Bulgarian authorities to swiftly prosecute violent attacks against journalists', *Organization for Security and Co-operation in Europe*, September 26, accessed at: http://www.osce.org/fom/50126

Owono J 2015 Qualitative interview conducted by Federica Cherubini for UNESCO Internet Study: Privacy and Journalists' Sources

Pacific Media Centre 2014, Timor Leste: Court of Appeal Again Declares Media Law Unconstitutional, December 17th. Accessed at: http://www.pmc.aut.ac.nz/pacific-media-watch/timor-leste-court-appeal-again-declares-media-law-unconstitutional-9089

Page K 2014, 'South African Government still funding Vastech, knows previous financing was for mass surveillance,' *Privacy International*, 30 January, accessed at: https://www.privacyinternational.org/?q=node/305

Palatino, M, 2014, *Philippine Supreme Court Upholds Cyber Libel Law*, Global Voices Advocacy, 19 February, accessed at: http://advocacy.globalvoicesonline.org/2014/02/19/philippine-supreme-court-upholds-cyber-libel-law/

Paletta D 2015, 'Yahoo executive confronts NSA director over 'backdoors'' *The Wall Street Journal*, 23 February, viewed 27 February 2015 at < http://blogs.wsj.com/washwire/2015/02/23/yahoo-executive-confronts-nsa-director-over-backdoors/>

Panam Post 2014, *Colombian Intelligence Chief Axed over Army Spying Scandal*, October 30, accessed at: http://panampost.com/panam-staff/2014/10/30/colombian-intelligence-chief-axed-over-army-spying-scandal/

Parliamentary Joint Committee on Intelligence and Security 2015, 'Advisory report on the Telecommunications (Interception and Access) Amendment Data Retention) Bill 2014,' Commonwealth of Australia, February, accessed at: http://www.aph.gov.au/~/media/02%20Parliamentary%20Business/24%20Committees/244%20Joint%20Committees/PJCIS/DataRetention2014/FinalReport_27February2015.pdf

PC World, 2014, *Austrian court axes data retention law following EU high court ruling*, June 27, accessed at: http://www.pcworld.com/article/2401520/austrian-court-axes-data-retention-law-following-eu-high-court-ruling.html

PEC Bill Pakistan, accessed at: http://bolobhi.org/wp-content/uploads/2015/04/NA-Standing-Committee-Version.pdf

Perlez J 2010, 'Pakistani Journalist Speaks Out After an Attack', *The New York Times*, September 24, accessed at: http://www.nytimes.com/2010/09/25/world/asia/25cheema.html?_r=2

Perlroth, N, 2013, 'Researchers Find 25 Countries using Surveillance Software', *New York Times*, March 23. Accessed at: http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/?gwh=619D5B69FD878BB23AFF2069495A5B47&gwt=pay

Peru21. "Norma mordaza contra difusión de audios". Accessed at: http://peru21.pe/noticia/851907/presentan-proyecto-contra-difusion-audios

Peruvian Computer Crimes Law 2013, accessed at: http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc02_2011_2.nsf/d99575da99ebfbe305256f2e006d1cf0/a8851de57eec4e8205257c0c004fc83d/$FILE/30096.pdf

Pilkington E, Rushe D 2015, 'WikiLeaks demands answers after Google hands staff emails to US government' *The Guardian*, 25 January, viewed 27 February. Accessed at: http://www.theguardian.com/technology/2015/jan/25/wikileaks-google-staff-emails-us-government

Pearson M 2013, "RWB welcomes creation of press council and code of ethics," *RSF*, 7 November, accessed at: http://en.rsf.org/east-timor-rwb-welcomes-creation-of-press-07-11-2013,45436.html

Pearson M and Fernandez, J (2015, forthcoming). *Censorship in Australia: intrusions into media freedom flying beneath the international free expression radar* Pacific Journalism Review, vol 21, issue 1.

Pheap A and Wilwohl J 2014, 'Gov't Plans to Install Surveillance Equipment', *The Cambodia Daily*, December 10, accessed at: https://www.cambodiadaily.com/archives/govt-plans-to-install-surveillance-equipment-73911/

Phillips G 2014, 'On protection of journalistic sources,' *Center for Media, Data and Society*, CEU School of Public Policy, 10 October, accessed at: http://journalism.cmpf.eui.eu/discussions/on-protection-of-journalistic-sources/

PMG. Protection Of State Information Bill (B6-2010), Parliamentary Monitoring Group; https://pmg.org.za/bill/278

Podkowik J 2014, 'Secret surveillance, national security and journalistic privilege – in search of the balance between conflicting values in the age of new telecommunication technologies,' University of Oslo. Accessed at: http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws8/w8-podkowik.pdf

POESY n.d. *Panhellenic Federation of Journalists' Unions* http://www.poesy.gr/

Ponsford D 2015a, 'Theresa May says Government is working through legal detail of Save Our Sources law ahead of Monday's Commons vote', *Press Gazette*, 18 February, viewed 27 February 2015 at: http://www.pressgazette.co.uk/theresa-may-says-government-working-through-legal-detail-save-our-sources-law-head-mondays-commons

Ponsford D 2015b *Rusbridger: Fractured Press Must Remember Sacred Oath to Protect Sources* http://www.pressgazette.co.uk/rusbridger-fractured-press-must-remember-sacred-oath-protect-sources-we-are-beginning-fight

Ponsford D 2015c, "Court set to decide whether Met Police broke the law by secretly grabbing Sun phone records," *Press Gazette*, 7 January, accessed at: http://ns337646.ip-5-196-77.eu/court-set-decide-whether-met-police-broke-law-secretly-grabbing-sun-phone-records

Ponsford D & Turvill W 2015, 'Two more journalists emerge as police spying targets, Press Gazette says: 'We've been misled by Met,' *Press Gazette*, 27 January, accessed at: http://www.pressgazette.co.uk/two-more-journalists-emerge-plebgate-police-ripa-targets-press-gazette-says-we-have-been-misled-met

Posetti J 2014a 'World Editors Forum Commissioned to Conduct Study on Protection Of Journalists' Sources', 4 September, *World News Publishing Focus*. Accessed at: http://blog.wan-ifra.org/2014/09/04/world-editors-forum-commissioned-by-unesco-to-conduct-study-on-the-protection-of-journali

Posetti J 2014b, 'One Year on: What's the impact of the Snowden-effect on your newsroom?' *World News Publishing Focus*, 20 June, accessed at: http://blog.wan-ifra.org/2014/06/20/one-year-on-whats-the-impact-of-the-snowden-effect-on-your-newsroom

Posetti, J, 2014c, 'The Urgent Need to Shield Journalism in the Age of Surveillance', *Trends in Newsrooms* 2014, World Editors Forum, Paris (See also: http://blog.wan-ifra.org/2014/06/24/trends-in-newsrooms-the-urgent-need-to-shield-journalism-in-the-age-of-surveillance)

Posetti J 2014d '"Is it possible to protect journalists' sources in the digital age?", survey asks?' *World News Publishing Focus* http://blog.wan-ifra.org/2014/10/27/is-it-possible-to-protect-journalists-sources-in-the-digital-age-survey-asks

Posetti J 2015a, 'Beware of curtailing freedom of expression in the name of #CharlieHebdo', *World News Publishing Focus*, 12 January, accessed at: http://blog.wan-ifra.org/2015/01/12/beware-of-curtailing-freedom-of-expression-in-the-name-of-charliehebdo

Posetti J 2015b 'The fight to #FreeAJStaff continues and Australia's press freedom credentials are challenged, as Peter Greste heads home', *World News Publishing Focus*, 2 February at http://blog.wan-ifra.org/2015/02/02/the-fight-to-freeajstaff-continues-and-australias-press-freedom-credentials-are-challenge

Posetti J 2015c, 'UNESCO considers protection of journalists' sources in the digital era', *World News Publishing Focus* 4 March at http://blog.wan-ifra.org/2015/03/04/unesco-considers-protection-of-journalists-sources-in-the-digital-era

Posetti J 2015d 'New research: 11-point plan for protecting journalism sources in the digital age', 3 June, *World News Publishing Focus* http://blog.wan-ifra.org/node/15926

Posetti J & Sparks J, 2014 'Journalists may face prison under proposed new Australian anti-terror legislation', *World News Publishing Focus*, 19 September, accessed at: http://blog.wan-ifra.org/2014/09/19/journalists-may-face-prison-under-proposed-new-australian-anti-terror-legislation

Press Gazette 2015, 'Culture secretary backs calls for RIPA law change to protect journalists' source before May general election,' *Press Gazette*, 5 February, viewed 27 February 2015 at: http://www.pressgazette.co.uk/culture-secretary-backs-calls-ripa-law-change-protect-journalists-sources-may-general-election

Privacy International 2014 *Statement of Grounds* IPT https://www.privacyinternational.org/sites/default/files/Final%20Grounds%20-%20GCHQ%20attacking%20providers_0.pdf

Professional Secrets of Journalists Law (Mexico City), accessed at: http://www.aldf.gob.mx/archivo-d6d138e94b0268bc0fd4b7f6e14fe6a1.pdf

Protection Of State Information Bill, 2010 (South Africa), accessed at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/d-za/dv/draft_final_bill_voted/draft_final_bill_voteden.pdf

Quinn B 2014, 'Vodafone gives Metropolitan police excess of journalists' data in error,' *The Guardian*, 25 November, accessed at: < http://www.theguardian.com/business/2014/nov/25/vodafone-metropolitan-police-met>

Radsch C 2015 Qualitative interview conducted by Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

Ramstad E 2012 'South Korea Court Knocks Down Online Real-Name Rule', *Wall Street Journal*, 24 August, accessed at: http://online.wsj.com/articles/SB10000872396390444082904577606794167615620

RDM Newswire 2015. 'Protection of State Information legislation will not contravene constitution' 18 October, accessed at: http://www.timeslive.co.za/politics/2015/10/18/Protection-of-State-Information-legislation-will-not-contravene-constitution

Reporters Committee For Freedom of the Press 2013 *Media Coalition Letter Regarding AP Subpoena*, May 14, accessed at https://www.rcfp.org/sites/default/files/Media%20coalition%20letter%20re%20AP%20subpoena.pdf

Rech M 2015 Qualitative interview conducted by Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

RSF (Reporters Sans Frontieres) 2015a *Morocco Call for Material Seized*. Accessed at: http://en.rsf.org/morocco-call-for-return-of-material-seized-17-02-2015,47586.html

RSF. (Reporters Sans Frontiers) 2015b *Pakistan Legislators Urged to Overhaul Draconian Cyber-crime Bill*. Accessed at: http://en.rsf.org/pakistan-legislators-urged-to-overhaul-23-04-2015,47801.html

RSF (Reporters Sans Frontieres) 2015c *Analysis of Pakistan's Cyber-crime Bill*. Accessed at: http://en.rsf.org/IMG/pdf/analysis_of_pakistan_s_cyber-crime_bill.pdf

RSF. (Reporters Sans Frontiers) 2015d, *Controversial security law provisions ruled unconstitutional*, 26 February. Accessed at: < http://en.rsf.org/kenya-rwb-alarmed-by-new-security-law-22-12-2014,47408.html>

RSF (Reporters Sans Frontieres) 2015e, 'Liberté provisoire pour Bob Rugurika', *Reporters Sans Frontieres*, 19 February. Accessed at: http://fr.rsf.org/burundi-la-justice-confirme-les-charges-04-02-2015,47540.html

RSF (Reporters Sans Frontieres) 2014a, *Law on Protection of Sources Buried?* 23 July. Accessed at: http://fr.rsf.org/france-loi-sur-le-secret-des-sources-31-07-2014,46731.html

RSF (Reporters Sans Frontieres) 2014b, *RWB's Recommendations on Morocco's Media Reform Bills*, 21 November. Accessed at: http://en.rsf.org/maroc-rwb-s-recommendations-on-morocco-s-21-11-2014,47260.html

RSF (Reporters Sans Frontieres) 2014c, *Honduran president threatens reporter at public event*, Reporters Sans Frontieres, July 17. Accessed at: http://en.rsf.org/honduras-honduran-president-threatens-17-07-2014,46646.html

RSF (Reporters Sans Frontiers) 2014d, World Press Freedom Index *Europe and the Balkans* http://rsf.org/index2014/en-eu.php

RSF (Reporters Sans Frontiers) 2014e 'Bolivian judge rules that Press Court, not Criminal Court, should hear 'spying' case'. Accessed at: http://en.rsf.org/bolivia-judge-rules-that-press-court-not-08-08-2014,46778.html

RSF (Reporters Sans Frontieres) 2014f ' 2014, 'Republika Srpska police violate confidentiality of sources', December 30, accessed at: http://en.rsf.org/bosnia-herzegovina-republika-srpska-police-violate-30-12-2014,47432.html

RSF (Reporters Sans Frontieres) 2014g, "*Sudan: Scoring high in censorship*". Accessed at: http://12mars.rsf.org/2014-en/2014/03/10/29/

RSF (Reporters Sans Frontieres) 2013a, National assembly passes amendment to computer crimes law, April 23, accessed at: http://en.rsf.org/costa-rica-government-pledges-cybercrime-law-09-11-2012,43664.html

RSF (Reporters Sans Frontieres) 2013b, Ecuador New media law – mix of good principles and bad provisions, June 14, accessed at: http://en.rsf.org/ecuador-new-media-law-mix-of-good-14-06-2013,44795.html

RSF (Reporters Sans Frontieres) 2013c, *Senate urged not to approve proposed new media law*, April 4, accessed at: http://en.rsf.org/burundi-senate-urged-not-to-approve-04-04-2013,44302.html

RSF (Reporters Sans Frontieres) 2012, *Canadian Journalist's Home Searched* http://en.rsf.org/canada-journalist-s-home-searched-16-03-2012,42140.html)

RSF (Reporters Sans Frontieres) 2011a, *Government Announces Schizophrenic Media Law*, August 29, accessed at: http://en.rsf.org/syria-government-announces-schizophrenic-29-08-2011,40870.html

RSF (Reporters Sans Frontieres) 2011b 'Charges dropped against freelance journalist Elena Bondar', 8 September, accessed at: http://en.rsf.org/ouzbekistan-freelance-journalist-elena-bondar-30-08-2011,40844.html

RSF (Reporters Sans Frontieres) 2011c *Questions raised by detention of four photographers* http://en.rsf.org/georgia-questions-raised-by-detention-of-08-07-2011,40622.html

RSF (Reporters Sans Frontieres) 2008, 'Judicial harassment forces Bishkek newspaper to suspend publishing', July 3, accessed at: http://archives.rsf.org/print.php3?id_article=27735

RSF (Reporters Sans Frontieres) (RSF)/IFEX, 2012, *New Costa Rican cybercrime law will not apply to journalists*, Reporters Sans Frontieres via IFEX, November 12, accessed at: https://www.ifex.org/costa_rica/2012/11/12/cybercrime_law/

Republica Democratica De Timor-Leste, 2013, *National Journalist Congress approves Code of Ethics*, Governo de Timor-Leste, October 28. Accessed at: http://timor-leste.gov.tl/?p=9238

Reuters 2011 '*Algeria lifts 19-year-old state of emergency*, February 24, accessed at: http://www.reuters.com/article/2011/02/24/us-algeria-emergency-lifting-idUSTRE71N6VS20110224

Rhanem K 2014 '*Morocco New Digital Code to Put an End to Online Anonymity*', Morocco World News, 25 March (Note: Link to official legislation has been removed after criticisms - http://www.moroccoworldnews.com/2014/03/126411/morocco-new-digital-code-to-put-an-end-to-online-anonymity/

Rhodes T 2015, 'Press law debate and journalist's release signal hope for Burundi's media,' *Committee to Protect Journalists*, March 10. Accessed at: https://cpj.org/blog/2015/03/hope-for-burundis-press-with-release-of-radio-dire.php

Rhodes T 2014 'Burundi's Journalists' Union Takes Repressive Press Law to Court' Committee to Protect Journalists. Accessed at: https://cpj.org/blog/2014/09/burundis-journalist-union-takes-repressive-press-l.php

Ria Novosti 2013, (РИА Новости), 'Wiretapping of telephone conversations and intercepting traffic in Russia' (Прослушка телефонных разговоров и перехват трафика в России), *Ria Novosti (РИА Новости),* August 15, accessed at: http://ria.ru/infografika/20130815/956535235.html

Rice K 2013 *Spy Bill Passed*, BizCommunity, June 14, accessed at: http://www.bizcommunity.com/Article/196/364/94958.html

Right 2 Know 2012, 'Guide: Why the secrecy Bill still fails the freedom test,' *Right 2 Know*, 28 November, accessed at: http://www.r2k.org.za/2012/11/28/guide-why-secrecy-bill-fails/

Right to 2 Know 2014 'R2K's Secret State of the Nation report – with infographics,' *Right 2 Know*, 9 September, accessed at: http://www.r2k.org.za/2014/09/09/r2k-secrecy-report-2014/

Rijksoverheid 2014 'Kabinet wijzigt regels dataretentie na uitspraak hof,' 18 November, viewed February 27 2015 at: http://www.rijksoverheid.nl/nieuws/2014/11/18/kabinet-wijzigt-regels-dataretentie-na-uitspraak-hof.html

Robertson G 2013 'Media law and ethics in Mauritius,' *GIS*, accessed at: http://gis.govmu.org/English/Documents/Media%20Law%20-%20Preliminary%20Report.pdf

Robinson M, 2011, 'Georgian photojournalists arrested for spying', *Reuters*, July 7, accessed at: http://www.reuters.com/article/us-georgia-photographers-arrest-idUSTRE7661GB20110707

Rodriguez K 2011 The Politics of Surveillance: The Erosion of Privacy in Latin America, *Electronic Frontier Foundation*, July 22, accessed at: https://www.eff.org/deeplinks/2011/07/politics-surveillance-erosion-privacy-latin-america

Ruane K A 2011, 'Journalists' privilege: Overview of the law and legislation in recent congresses' *CRS Report for Congress*, 19 January, viewed 27 February 2015 at https://www.fas.org/sgp/crs/secrecy/RL34193.pdf

Ruiz C, 2010, Chile: First Country to Legislate Net Neutrality, Global Voices, September 4, accessed at: https://globalvoices.org/2010/09/04/chile-first-country-to-legislate-net-neutrality/

Rusbridger A 2015 Qualitative interview conducted by Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

Russell L 2014, "Shielding the Media: In an Age of Bloggers, Tweeters, and Leakers, Will Congress Succeed in Defining the Term "Journalist" and in Passing a Long-Sought Federal Shield Act?" Oregon Law Review, 93, pp 193-227

Ryle, G 2015 Qualitative interview conducted by Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

s.1599, 113th Congress 2013 – 2014, accessed at: https://www.congress.gov/bill/113th-congress/senate-bill/1599

Sabbagh, R 2015 Qualitative interview conducted by Farrah Wael for UNESCO Internet Study: Privacy and Journalists' Sources

SABC 2013, 'National Assembly approves info Bill,' SABC NEWS, 12 November, accessed at: http://www.sabc.co.za/news/a/8612bb8041cd7c3e8bd9cb5393638296/National-Assembly-approves-Info-Bill-20131211

Siddiqui S 2015, «Congress passes NSA surveillance reform in vindication for Snowden, » *The Guardian*, 3 June, accessed at : < http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden>

Said B 2015 Email to Julie Posetti June 26th

SANEF 2010a 'SANEF appalled that section 205 of the Criminal Procedure Act has been invoked against journalists,' *South African National Editors' Forum*, 'http://www.sanef.org.za/news/entry/sanef_appalled_that_section_205_of_the_criminal_procedures_act_has_been_inv/

SANEF 2010b 'Sanef calls for police and prosecuting authorities to withdraw Section 205 subpoenas', South Africa National Editors Forum, accessed at: http://www.sanef.org.za/news/entry/sanef_calls_for_police_and_prosecuting_authorities_to_withdraw_section_205_/

SANEF 2012, 'Sanef welcomes court decision that journalists are not obliged to reveal their sources' *South African National Editors' Forum*, accessed at: http://www.sanef.org.za/news/entry/sanef_welcomes_court_decision_that_journalists_are_not_obliged_to_reveal_th/

Sapo Notícias 2014, 'Parlamento timorense aprova por unanimidade alterações à lei da comunicação social' *Sapo Notícias* 27 October, accessed at: 'http://noticias.sapo.tl/portugues/lusa/artigo/18419360.html

Saul, H 2013, 'Kenyan soldiers are jailed for looting mall during Westgate attack', *The Independent*, October 29, accessed at: http://www.independent.co.uk/news/world/africa/kenyan-soldiers-are-jailed-for-looting-mall-during-westgate-attack-8911129.html

Savage C & Kaufman L 2013, " Phone records of journalists seized by US," *The New York Times*, 13 May, accessed at: < http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html?pagewanted=all>

Savage C 2014a, "Ex-contractor at state department pleads guilty in leak case," *The New York Times*, 7 February, accessed at: < http://www.nytimes.com/2014/02/08/us/politics/ex-state-department-contractor-pleads-guilty-in-leak-case.html>

Savage C 2014b, "Attorney General Signs New Rules to Limit Access to Journalists' Records," *The New York Times*, 21 February, accessed at: < http://www.nytimes.com/2014/02/22/us/attorney-general-signs-new-rules-to-limit-access-to-journalists-records.html?_r=0>

Sayadyan L 2014, 'AEJ Austria 2014 Congress media freedom report: Armenia' *Association of European Journalists*, viewed 27 February 2015 at <http://www.aej.org/articlefiles/aej%20austria%202014%20congress%20armenia%20media%20freedom%20report.pdf>

Sazanova-Prokouran 2015, 'Le Monde Afrique's first week in review' *WAN IFRA*, 29 January, viewed 27 February 2015, accessed at: < http://blog.wan-ifra.org/2015/01/29/le-monde-afriques-first-week-in-review>

Scahill J, Begley J 2015, 'The great sim heist: How spies stole the keys to the encryption castle,' *The Intercept*, 19 February, viewed 27 February 2015 at https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

SCC 2010 16 R v *National Post* http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7856/index.do

Senado Federal, 2014 '*Communication Council approves requirement journalist diploma*', Senado Notícias, August 6, accessed at: http://www12.senado.leg.br/noticias/materias/2014/08/06/conselho-de-comunicacao-aprova-exigencia-do-diploma-de-jornalista

Stichting Ostade Blade v The Netherlands in the ECtHR 2014 (Application no. 8406/06): Stichting Ostade Blade v The Netherlands in the ECtHR 2014 (Application no. 8406/06), *European Court of Human Rights*, 27 May, accessed at: < http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-145098>

Shah N 2015, "8 Facts You Need to Know: Why We're Suing to Stop Surveillance – and Protect Human Rights," *Amnesty International USA*, 10 March, accessed at: <http://blog.amnestyusa.org/us/8-facts-you-need-to-know-why-were-suing-to-stop-surveillance-and-protect-human-rights/>

Shahid J 2014, 'No safeguards to protect people from govt snooping', *Dawn.com*, 15 November, accessed at: http://www.dawn.com/news/1144575

Sherman, M, 2013, *Gov't obtains wide AP phone records in probe*, The Associated Press, May 13, accessed at: http://bigstory.ap.org/article/govt-obtains-wide-ap-phone-records-probe

Shiv Malik v Attorney General [2008] EWHC 1362): Shiv Malik v Attorney General [2008] EWHC 1362, accessed at: <http://www.bailii.org/ew/cases/EWHC/Admin/2008/1362.html >

Sihaloho, Markus Junianto, 2012, "Constitutional Court rejects appeal of intelligence law", *Jakarta Globe*, 11 October, available at URL: http://thejakartaglobe.beritasatu.com/archive/constitutional-court-rejects-appeal-of-intelligence-law/

Simon J 2009, '*Liberian journalist will not have to reveal source,' Committee to Protect Journalists*, Feb 19, accessed at: https://cpj.org/blog/2009/02/liberian-journalist-will-not-have-to-reveal-source.php

Simmons, R, 2012, *Martínez solicita el retiro del proyecto 377 sobre internet*, La Prensa, October 4, accessed at: http://www.prensa.com/uhora/locales/martinez-solicita-el-retiro-del-proyecto-377-sobre-internet/128253

Smith v Maryland 442 US 735 Supreme Court 1979, accessed at: http://scholar.google.com/scholar_case?case=3033726127475530815&hl=en&as_sdt=6&as_vis=1&oi=scholar

Smith D 2013 'South Africa secrecy law surprise as Zuma rejects controversial bill', *The Guardian*, September 13, accessed at: http://www.theguardian.com/world/2013/sep/12/south-africa-zuma-secrecy-bill

Smith R 2010 'Reflections on the Icelandic Modern Media Initiative: A Template for Modern Media Law Reform?' *Journal of Media Law*, 2(2) 199–211

Soendergaard M 2014 'DAS wiretapping scandal', *Fact Sheets, Colombia Reports*, February 24. Accessed at: http://colombiareports.co/das-colombia-wiretapping-scandal

Soldatov A, Borogan I 2013, 'Russia's Surveillance State' *World Policy Institute*, viewed February 27 February 2015, at: http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Sparrow A 2015, 'No 10 hints it will reject key proposal in David Anderson's surveillance report - Politics live,' *The Guardian*, 11 June, accessed at: <http://www.theguardian.com/politics/blog/live/2015/jun/11/david-anderson-terror-watchdog-publishes-report-on-surveillance-powers-politics-live#block-55797ac0e4b0d852ce137581>

Spiegel M 2012, 'Smoke and Mirrors: Malaysia's 'new' Internal Security Act' *Asia Pacific Bulletin*, 14 June, No.167, accessed at: http://www.hrw.org/sites/default/files/related_material/2012_Malaysia_EastWest.pdf

Spiegel Online International 2008, 'Big Brother Worries: German Parliament Passes Anti-Terror Law,' *Spiegel Online International*, 13 November, accessed at: <http://www.spiegel.de/international/germany/big-brother-worries-german-parliament-passes-anti-terror-law-a-590198.html>

Spiegel Online International 2013, 'Snowden Document: NSA Spied On Al Jazeera Communications' *Der Spiegel*, 31 August. Accessed at: http://www.spiegel.de/international/world/nsa-spied-on-al-jazeera-communications-snowden-document-a-919681.html

Sri Lanka: Law No. 5 of 1973, Press Council Law [Sri Lanka], Chapter 378, 30 May 1973. Accessed at: http://www.refworld.org/docid/4be018692.html

Stearns, Josh, 2013, *Acts of journalism: Defining Press Freedom in the Digital Age*, Free Press: Washington DC available online: http://www.freepress.net/resource/105079/acts-journalism-defining-press-freedom-digital-age

Stahl L 2014, 'The war on leaks' *CBS News*, 12 October. Accessed at: <http://www.cbsnews.com/news/war-on-leaks-national-security-press-freedom/>

Stearns, J (2015) Qualitative interview conducted by Marcus O'Donnell for UNESCO Internet Study: Privacy and Journalists' Sources

Stichting Ostade Blade v The Netherlands in the ECtHR 2014 (Application no. 8406/06): Stichting Ostade Blade v The Netherlands in the ECtHR 2014 (Application no. 8406/06), *European Court of Human Rights*, 27 May, accessed at: < http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-145098>

Sudan, 2010. National Security Act قنسل يئنطولا نمألا نوناق Republic of Sudan; http://moj.gov.sd/content/lawsv4/12b/10.htm

Sun Daily 2010, 'Challenge to SC withdrawn', *The Sun Daily*, 9 July. Accessed at: http://www.thesundaily.my/node/140985

Supreme Court of the Russian Federation, 2010, *On practice of application by the courts of the Law of the Russian Federation On mass media*, June 15, accessed at: https://cpj.org/blog/RussianSCResolution.pdf

Supremo Tribuno Federal, 2009 (Brasil), *Supreme Court Decides it's unconstitutional the degree requirement for the practise of journalism*, June 17. Accessed at: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=1097

Suzor N, Button-Sloan A 2014, 'When does Google hand over your data to governments?' *The Conversation*, 19 September: http://theconversation.com/when-does-google-hand-over-your-data-to-governments-31779

Szymielewic K & Walkowiak A, 2014 'Access to telecommunication data in Poland: Specific problems and general conclusions,' *Gis Watch*. Accessed at: <http://www.giswatch.org/en/country-report/communications-surveillance/poland#_ftn4>

Tapper J 2015, 'Obama administration spied on German media as well as its government,' *CNN*, 4 July, accessed at: < http://edition.cnn.com/2015/07/03/politics/germany-media-spying-obama-administration/index.html?utm_source=Daily+Lab+email+list&utm_campaign=3fe153bb96-dailylabemail3&utm_medium=email&utm_term=0_d68264fd5e-3fe153bb96-395894269>

Tate J 2013, 'Bradley Manning sentenced to 35 years in WikiLeaks case,'*The Washington Post*, 21 August. Accessed at: < https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html>

Telegraaf Media Nederland Landelijke Media b.v. and others v. the Netherlands (Application no. 39315/06): Telegraaf Media Nederland Landelijke Media b.v. and others v. the Netherlands 2013 (Application no. 39315/06), *European Court of Human Rights*, 22 February, accessed at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-114439

Telecommunications, Information Technology and Communication Law 2011 (Bolivia). Accessed at: http://www.andi.org.br/sites/default/files/legislacao/Ley%20de%20telecomunicaciones%20de%20Bolivia_0.pdf

Telecommunication Regulator of Cambodia, 2014, 'Letter of telecommunication regulators' *Kingdom of Cambodia*, December. Accessed at: https://www.cambodiadaily.com/cdfiles/wp-content/uploads/2014/12/letter-of-telecommunication-regulators.pdf

Telecommunications (Interception and Access) Act 1979 (Cth), No114, Chapter 2, *Parliament of Australia*. Accessed at: http://www.comlaw.gov.au/Details/C2013C00361

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 *Parliament of Australia*, Accessed at: <http://parlinfo.aph.gov.au/parlInfo/download/legislation/amend/r5375_amend_bb5b4d2f-8bf3-4654-8df5-b4095d7d3ee0/upload_pdf/GT140.pdf;fileType=application%2Fpdf>

Telecommunication Regulator of Cambodia 2014, letter dated 7 October 2014 as published by *The Cambodia Daily*, December 10, accessed at: https://www.cambodiadaily.com/cdfiles/wp-content/uploads/2014/12/letter-of-telecommunication-regulators.pdf

Telstra n.d. 'Transparency at Telstra', accessed at: http://www.telstra.com.au/privacy/transparency

The Constitution of Zimbabwe Amendment (No. 20) Act 2003, made available by the official website of the Ministry of Justice, Legal and Parliamentary Affairs of Zimbabwe, accessed at: http://www.justice.gov.zw/index.php/downloads

The Economist 2010, '*Le Monde* reignites the Bettencourt Affair' *The Economist*, 14 September, accessed at: http://www.economist.com/blogs/newsbook/2010/09/le_monde_and_bettencourt_affair

The Economist 2015, 'Why locking up leakers makes sense,' *The Economist*, 29 January, viewed 5 February 2015, accessed at: http://www.economist.com/blogs/democracyinamerica/2015/01/press-freedom-and-national-security

The General Intelligence Laws Amendment Bill (GILAB) 2013 (South Africa). Accessed at: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf

The Guardian 2015, 'The NSA Files'. Accessed at: http://www.theguardian.com/us-news/the-nsa-files

The Guardian 2015, 'Egypt drops two-year jail penalty for journalists in proposed anti-terror law', *The Guardian*, 16 July, accessed at: http://www.theguardian.com/world/2015/jul/16/egypt-drops-two-year-jail-penalty-for-journalists-in-proposed-anti-terror-law

The Jamaica Gleaner 2011, 'Argentina Targets Reporting Of Inflation Data', 25 September. Accessed at: http://jamaica-gleaner.com/gleaner/20110925/business/business2.html

The New York Times, 2015, 'Lessons of the James Risen Case' 22 January. Accessed at: <http://www.nytimes.com/2015/01/22/opinion/lessons-of-the-james-risen-case.html?_r=0>

The Press and Printed Materials Act 2009 (Sudan). Accessed at: http://www.icnl.org/research/library/files/Sudan/pressprin.pdf

The Security Laws (amendment) Act 2014, Kenya Gazette, 22 December. Accessed at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf

Therrien D 2015, 'Statement from the Privacy Commissioner of Canada following the tabling of Bill C-51,' *Office of the Privacy Commissioner of Canada*, 30 January 2015, accessed at: https://www.priv.gc.ca/media/nr-c/2015/s-d_150130_e.asp

Tillack v Belgium (20477/05) 2008, *European Court of Human Rights*, 27 February. Accessed at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-83527

Times Live 2013, 'Police illegally tapped journalists phones: Report' *Times Live*, 18 August, accessed at: http://www.timeslive.co.za/local/2013/08/18/police-illegally-tapped-journalists-phones-report

Timor Leste Press Law, 2014, Article 2, a) Decree No. 10/III Media Act. Accessed at: http://www.hrw.org/news/2014/07/15/timor-leste-press-law-2

Tobin, C, 2015 Qualitative interview conducted by Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

Travis A 2015, "Security services capable of bypassing encryption, draft code reveals," *The Guardian*, 6 February, accessed at: http://www.theguardian.com/uk-news/2015/feb/06/uk-security-services-capable-bypassing-encryption-draft-code

Trehoring, Par Qualitative interview conducted via phone by Angelique Lu and Julie Posetti January 27th, 2015

Tryhorn, C (2009) 'Court Rules in favour of news groups over Interbrew leaked documents' in *The Guardian* December 15th, 2009. Accessed at: http://www.theguardian.com/media/2009/dec/15/court-rules-interbrew-leaked-documents

Turkey, 2014. Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanunu, no. 6532; Republic of Turkey. Accessed at: http://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm

Turvill, W., & Ponsford, D., 2014, Met conducted 38 press leak investigations in five years - RIPA used in 'vast majority', says source, *Press Gazette*, October 24, accessed at: http://www.pressgazette.co.uk/met-conducted-38-press-leak-investigations-five-years-ripa-used-vast-majority-says-source

Turvill W, 'Guardian, Independent and Times join Mail on Sunday, Sun and Daily Telegraph in condemning RIPA use against journalists,' *The Press Gazette*, 9 October. Accessed at: <http://www.pressgazette.co.uk/guardian-and-times-join-mail-sunday-sun-and-daily-telegraph-condemning-ripa-use-against-journalists>

Turvill W 2015, 'Interception Commissioner: 82 journalists' phone records grabbed by police in three years, judicial oversight needed', *Press Gazette*, 4 February, viewed 27 February at: http://www.pressgazette.co.uk/interception-commissioner-82-journalists-phone-records-targeted-police-three-years-forces-should

Turvill W 2015, "Warning from media lawyers that journalists' sources are still at risk from police records grabs," *Press Gazette*, 8 May, accessed at: http://www.pressgazette.co.uk/warning-media-lawyers-journalists-sources-are-still-risk-police-records-grabs

Uganda 2002. The Anti-Terrorism Act, 2002. Accessed at: www.vertic.org/media/National Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf

UK Government 2015 *Draft Equipment Interference Code of Practice* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf

UK High Court 2015 Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014 https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf

UN 2003 *United Nations Convention Against Corruption* United Nations Office on Drugs and Crime. Accessed: http://www.whistleblowers.org/storage/whistleblowers/documents/internationalhomepage/un%20convention%20against%20corruption.pdf).

UN 2012, *UN experts raise concerns over 'landmark' Southeast Asian human rights declaration*, November 16, Accessed at: http://www.un.org/apps/news/story.asp?NewsID=43520#.Vqd5SZUQWJA ;

UN 2013a General Assembly Adopts 68 Resolutions, 7 Decisions as It Takes Action on Reports of Its Third Committee, December 18. Accessed at: http://www.un.org/press/en//2013/ga11475.doc.htm

UN 2013b Human Rights chief urges respect for right to privacy and protection of individuals revealing human rights violations, July 12. Accessed at: http://www.unmultimedia.org/radio/english/2013/07/human-rights-chief-urges-respect-for-right-to-privacy-and-protection-of-individuals-revealing-human-rights-violations/

UN General Assembly 2013, The safety of journalists and the issue of impunity : resolution / adopted by the General Assembly , 18 December 2013, A/RES/68/163, [accessed 8 March 2015]. Accessed at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/163

UN General Assembly 2014, The safety of journalists and the issue of impunity : resolution / adopted by the General Assembly , 18 December 2014, A/RES/69/185, [accessed 21 September 2015]. Accessed at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/185

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, [accessed February 2015]. Accessed at: http://www.refworld.org/docid/3ae6b3aa0.html

UN General Assembly, *International Covenant on Civil and Political Rights*, *ARTICLE 19*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: http://www.refworld.org/docid/3ae6b3aa0.html

UN General Assembly, *Universal Declaration of Human Rights*, *article 19*, article 12, 10 December 1948, 217 A (III), available at: http://www.refworld.org/docid/3ae6b3712c.html

UN Human Rights Council 2013, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40, available at: http://www.refworld.org/docid/51a5ca5f4.html [accessed 28 February 2015]

UN Human Rights Council 2014 *Discussion on the safety of journalists: Report of the Office of the United Nations High Commissioner for Human Rights*, 23 July 2014, A/HRC/27/35. Available at: http://www.refworld.org/docid/53eb46d34.html [accessed 22 November 2014]

UN Human Rights Council, *Safety of journalists: resolution/adopted by the Human Rights Council*, 9 October 2012, A/HRC/RES/21/12. Accessed at: http://www.refworld.org/docid/50adf4812.html

UNESCO 2013 *Resolution on Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society*, General Conference, 37th Session, November. Accessed at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf and http://unesdoc.unesco.org/images/0022/002261/226162e.pdf

UNESCO 2014a Contract for research services between UNESCO and WAN-IFRA

UNESCO 2014b *UNESCO Internet Study*. Accessed at: http://www.unesco.org/new/en/internetstudy accessed 23.11.14

UNESCO 2014c *World Trends in Freedom of Expression and Media Development* (UNESCO Publishing) http://unesdoc.unesco.org/images/0022/002270/227025e.pdf

US Bureau of Democracy, Human Rights and Labor 2012, 'Country Reports on Human Rights Practices for 2012 – Georgia,' *US Department of State*, viewed 27 February 2015, accessed at: http://www.state.gov/j/drl/rls/hrrpt/2012humanrightsreport/index.htm?year=2012&dlid=204287#wrapper

US Court of Appeal US v Lavabit (Under Seal). Accessed at: https://www.documentcloud.org/documents/981194-lavabit-proceedings-unsealed.html

US District Court 2013a EFF v US Government, Order against National Security Letters https://www.eff.org/files/filenode/nsl_order_scan.pdf

US District Court 2013b EFF v US Government. Order enforcing National Security Letters https://www.eff.org/files/2014/01/16/008_-redacted_order_enforcing_nsls_1165.pdf

US District Court of Columbia 2013c *Klayman v Obama Civil Act No. 13-0851(RJL)* December 1, 2013. Accessed at: https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48

Vaca Villareal, P (2015) Qualitative interview conducted by Alice Matthews for UNESCO Internet Study: Privacy and Journalists' Source

Vahlberg, A 2015 Qualitative interview conducted by Angelique Lu & Julie Posetti for UNESCO Internet Study: Privacy and Journalists' Sources

Vargas, O 2014, 'Nuevas disposiciones a la ley del secreto profesional del periodista' *Noticieros Televisa*, 11 September, viewed 27 Februar 2015. Accessed at: < http://noticieros.televisa.com/mexico-df/1409/nuevas-disposiciones-ley-secreto-profesional-periodista/

Voorhoof, D 2015 Qualitative interview conducted by Federica Cherubini for UNESCO Internet Study: Privacy and Journalists' Sources

WAN-IFRA 2008, 'Kyrgyzstan: newspaper forced to stop publication, pressure from authorities', *World Association of News Papers and News Publishers Editors Blog*, July 4, accessed at: http://www.editorsweblog.org/2008/07/04/kyrgyzstan-newspaper-forced-to-stop-publication-pressure-from-authorities

Warren, Aiden & Dirksen, Alexander 2014: 'Augmenting State Secrets: Obama's Information War,' *Yale Journal of International Affairs*, 9:1, 68-84

Weber D 2013, 'Gina Rinehart ordered to pay Fairfax journalist Adele Ferguson's legal costs,' *Australian Broadcasting Corporation*, 15 March, accessed at: <http://www.abc.net.au/news/2014-03-15/rinehart-ordered-to-pay-journalist27s-costs/5323084>

Wigmore 1923 *A treatise on the Anglo-American system of evidence in trials at common law: Including the statutes and judicial decisions of all jurisdictions of the United States and Canada* 2nd ed. Boston: Little Brown and Co.

Wikimedia et al Vs NSA Case 1:15-cv-00662-RDB https://www.aclu.org/files/assets/wikimedia_v2c_nsa_-_complaint.pdf

Williams SC G 2015 Qualitative interview conducted by Marcus O'Donnell for UNESCO Internet Study: Privacy and Journalists' Sources

Willsher K 2013, 'French officials can monitor internet users in real time under new law,' *The Guardian*, 11 December, accessed at: <http://www.theguardian.com/world/2013/dec/11/french-officials-internet-users-real-time-law>

Wise L, Landay J 2013, 'Government could use metadata to map your every move' *Electronic Frontier Foundation*, June 20, viewed on 15 February 2015, accessed at: https://www.eff.org/mention/government-could-use-metadata-map-your-every-move

Woolf N 2015, 'Barrett Brown sentenced to 63 months for 'merely linking to hacked material,' *The Guardian*, 22 January. Accessed at: < http://www.theguardian.com/technology/2015/jan/22/barrett-brown-trial-warns-dangerous-precedent-hacking-sentencing>

Xinhua News Agency 2014 China Regulates Instant Messaging Services Accessed at: http://news.xinhuanet.com/english/china/2014-08/07/c_133539676.htm

York, J (2015) Qualitative interview conducted by Farrah Wael for UNESCO Internet Study: Privacy and Journalists' Sources

Yuhas A 2015, 'NSA reform: USA Freedom Act passes first surveillance reform in decade – as it happened,' 2 June. Accessed at: < http://www.theguardian.com/us-news/live/2015/jun/02/senate-nsa-surveillance-usa-freedom-act-congress-live>

Zadock, A 2013, 'Westgate: Kimaiyo now threatens journalists' *Daily Nation*, October 23, accessed at: http://www.nation.co.ke/news/Reporters-face-arrest-for-exposing-Westgate-looting/-/1056/2044972/-/3upkxcz/-/index.html

Zhen, Y (pseudonym) (2015) Qualitative interview conducted by Ying Chan for UNESCO Internet Study: Privacy and Journalists' Sources

Zheng W Y (2015) Qualitative interview conducted by Ying Chan for UNESCO Internet Study: Privacy and Journalists' Sources.

Appendices

Appendix 1: List of experts accessed for qualitative interviews*

	Interviewee	Title/Expertise	Gender	Region/ Country	Interviewer
1.	Charles Tobin	Legal expert, attorney	Male	Europe/North America (US)	Julie Posetti
2	Gavin Millar QC	Media law expert, Queens Counsel (QC)	Male	Europe/North America (UK)	Julie Posetti
3	Dr Courtney Radsch	Committee to Protect Journalists, Advocacy Director	Female	Europe/North America (US)/ GLOBAL	Julie Posetti
4	Alan Rusbridger	Editor-in-Chief *The Guardian*	Male	Europe/North America (UK)	Julie Posetti
5	Gerard Ryle	Director International Consortium of Investigative Journalists (ICIJ)	Male	Europe/North America (US)/ GLOBAL	Julie Posetti
6	Marty Baron	Editor-in-Chief, The Washington Post	Male	Europe/North America (US)	Julie Posetti
7	Marites Danguilan Vitug	Philippines Centre for Investigative Journalism	Female	Asia/Pacific (Philippines)	Angelique Lu
8	Peter Noorlander	Media Lawyer, Media Legal Defence Initiative (MLDI)	Male	Europe/North America (UK)/ GLOBAL	Emma Goodman
9	Jillian York	Executive Director, Electronic Frontier Foundation (EFF)	Female	Europe/North America/ GLOBAL	Farah Wael
10	Susan E McGregor	Tow Centre, Columbia University (academic)	Female	Europe/North America (US)	Angelique Lu
11	Fredrik Laurin (two interviews conducted)	Director Investigative Unit, Swedish Public Radio (SR)	Male	Europe/North America (Sweden)	Federica Cherubini Angelique Lu & Julie Posetti

12	Gunnar Nygren	Professor, Journalism, Södertörn University	Male	Europe/North America (Sweden)	Angelique Lu
13	Amare Aregawi	Journalist	Male	Africa (Ethiopia)	Federica Cherubini
14	Prof Dirk Voorhoof	Media-Law academic, University of Ghent	Male	Europe/North America (Belgium)	Federica Cherubini
15	Umar Cheema	Investigative journalist/ Co-founder Pakistan Centre for Investigative Reporting	Male	Asia/Pacific (Pakistan)	Federica Cherubini
16	George Williams SC	Constitutional law expert, University of NSW	Male	Asia/Pacific (Australia)	Marcus O'Donnell
17	Prof Wendy Bacon	Journalism academic/ investigative journalist/ Australian Centre for Independent Journalism	Female	Asia/Pacific (Australia)	Marcus O'Donnell
18	Peter Bartlett QC	Media lawyer, barrister	Male	Asia/Pacific (Australia)	Marcus O'Donnell
19	Leanne O'Donnell	Digital media lawyer	Female	Asia/Pacific (Australia)	Marcus O'Donnell
20	Josh Stearns	Journalist/Press freedom activist	Male	Europe/North America (US)	Marcus O'Donnell
21	Toby Mendel	Centre for Law and Democracy, Director	Male	Europe/North America (Canada)/ Global	Marcus O'Donnell
22	Tomaso Falchetta	Privacy International, legal policy officer	Male	Europe/North America (UK)/ Global	Emma Goodman
23	Julie Owono	Internet Without Borders	Female	Africa (Cameroon)/ Global	Federica Cherubini
24	Dr Justine Limpitlaw	Legal expert	Female	Africa (South Africa)	Angelique Lu
25	Javier Gaza Ramos	Journalism security & safety expert	Male	Latin America (Mexico)	Jake Evans

26	Rana Sabbagh	Investigative journalist/ Executive Director, Arab Reporters for Investigative Journalism (ARIJ)	Female	Arab States (Jordan)/ Regional	Farah Wael
27	Anita Vahlberg	Senior Advisor, Swedish Union of Journalists	Female	Europe/North America (Sweden)	Angelique Lu/Julie Posetti
28	Pär Trehörning	Lawyer advising Swedish Union of Journalists/Press Ombudsman	Male	Europe/North America (Sweden)	Angelique Lu/Julie Posetti
29	Katarina Berglund-Siegbahn	Constitutional Law Expert, Swedish Department of Justice	Female	Europe/North America (Sweden)	Julie Posetti
30	Toyosi Ogunseye	Investigative journalist, The Star	Female	Africa (Nigeria)	Federica Cherubini
31	Marcelo Rech	Globo RBS, Director of Journalism/Chair, World Editors Forum	Male	Latin America (Brazil)	Julie Posetti
32	Prof Ronaldo Lemos	Director of the institute for technology and society of Rio de Janeiro (ITS) and a law professor at the Rio de Janeiro State University	Male	Latin America (Brazil)	Carlos Affonso Souza
33	Carlos Guyot	Editor-in-Chief, La Nacion	Male	Latin America (Argentina)	Alice Matthews
34	Pedro Vaca Villareal	Executive Director Ejecutivo en Fundación para la Libertad de Prensa (FLIP)	Male	Latin America (Colombia)	Alice Matthews
35	Dr Catalina Botero	Special Rapporteur Freedom of Expression: Inter-American Commission on HR; lawyer	Female	Latin America (Columbia)/ Regional expert	Alice Matthews
36	Zine Cherfauoi	Editor-in-Chief Al Watan	Male	Arab States (Algeria)	Alexandra Waldhorn

37	Rawda Ahmed	Arabic Network for Human Rights & Information	Female	Arab States (Egypt)	Alexandra Waldhorn
38	Cliff Buddle	Senior Editor South China Morning Post	Male	Asia/Pacific, China (Hong Kong)	Doreen Weisenhaus
39	Daoud Kuttab	Journalist	Male	Arab States (Jordan)/	Alexandra Waldhorn
40	Rasha Abdulla	Professor Media Studies American University Cairo	Female	Arab States (Egypt)	Alexandra Waldhorn
41	Prof Wei Yong Zheng	Professor of Media Law at the University of China in Beijing	Male	Asia/Pacific (China)	Ying Chan
42	Mahasen Al Eman	Director Arab Women's Media Centre	Female	Arab States (Jordan)/	Alexandra Waldhorn
43	Ricardo Aguilar	Investigative Journalist, La Razon	Male	Latin America (Bolivia)	Alice Matthews
44	Silvia Higuera	Knight Centre for the Americas	Female	Latin America (Columbia)/	Alice Matthews
45	Henry Maina	Article 19, East Africa	Male	Africa (Kenya)	Alexandra Waldhorn
46	Yuan Zhen (pseudonym)	Editor-in-Chief (Unnamed newspaper)	Male	ASIA/Pacific (China)	Ying Chan
47	Yves Eudes	Investigative journalist/Le Monde; Co-founder SourceSure	Male	Europe/North America (France)	Alexandra Sazanova-Prokrouran
48	Atanas Tchobanov	Editor-in-Chief, Bivol/ Balkanleaks	Male	Europe/North America (Bulgaria)	Alexandra Sazanova-Prokrouran
49	Prof Hans-Gunnar Axberger	Professor of Constitutional Law at the University of Uppsala	Male	Europe/North America (Sweden)	Caroline Hammarberg

* *Designations correct at mid-2015*

*** Gender breakdown: 44% female*

Appendix 2: List of review panel members[24* 25**]

REVIEW PANEL MEMBER	AFFILIATION
1. Professor Mark Pearson (media law/ digital journalism expert)	Griffith University AUSTRALIA
2. Dr Julie Reid (media studies in Africa expert)	UNISA (University of South Africa) SOUTH AFRICA
3. Lillian Nalwoga (African ICT policy expert)	President of the Internet Society's Uganda Chapter; Policy Officer at the Collaboration on International ICT Policy in East and Southern Africa (CIPESA); coordinator of the Uganda and East African Internet Governance Forums. UGANDA
4. Dan Gillmor (journalism professor and international digital media expert)	Dan Gillmor is Professor of Practice, Walter Cronkite School of Journalism and Mass Communication, Arizona State University. UNITED STATES OF AMERICA
5. Prisca Orsonneau (barrister, legal expert in press freedom matters)	Lawyer at the Paris Bar, specializing in Media Law and Human Rights. Chair of the Reporters Without Borders Legal Committee. FRANCE
6. Gayathry Venkiteswaran (Press organization represenative)	Executive Director, Southeast Asian Press Alliance THAILAND
7. Mario Calabresi (newspaper editor)	Editor-in-Chief, La Stampa; World Editors Forum board member ITALY
8. Mishi Choudhary (international digital law expert)	Legal Director, Software Freedom Law Centre and SFLC.in INDIA

24 * Designations as at mid-2015
25 ** Gender breakdown: 63% female

UNESCO Series on Internet Freedom (cont.)

Fostering freedom online: the role of internet intermediaries

With the rise of Internet intermediaries that play a mediating role between authors of content and audiences on the internet, this UNESCO publication provides in-depth case studies and analysis on how internet intermediaries impact on freedom of expression and associated fundamental rights such as privacy. It also offers policy recommendations on how intermediaries and states can improve respect for internet users' right to freedom of expression.

Global survey on internet privacy and freedom of expression

This publication seeks to identify the relationship between freedom of expression and Internet privacy, assessing where they support or compete with each other in different circumstances. The book maps out the issues in the current regulatory landscape of Internet privacy from the viewpoint of freedom of expression. It provides an overview of legal protection, self-regulatory guidelines, normative challenges, and case studies relating to the topic. .

Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet

This report provides a new perspective on the social and political dynamics behind the threats to expression. It develops a conceptual framework on the 'ecology of freedom of expression' for discussing the broad context of policy and practice that should be taken into consideration in discussions of this issue.

All publications can be downloaded at:
http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/

Protecting Journalism Sources in the Digital Age

This comprehensive study highlights changes that impact on legal frameworks that support protection of journalistic sources in the digital age. This research responds in part to a UNESCO resolution by the 38th General Conference held in 2015 as well as the CONNECTing the Dots Outcome Document adopted by our 195 Member States that same year.

While the rapidly emerging digital environment offers great opportunities for journalists to investigate and report information in the public interest, it also poses particular challenges regarding the privacy and safety of journalistic sources. These challenges include: mass surveillance as well as targeted surveillance; data retention; expanded and broad anti-terrorism measures and national security laws; and over-reach in the application of these. All these can undermine the confidentiality protection of those who collaborate with journalists, and who are essential for revealing sensitive information in the public interest but who could expose themselves to serious risks and pressures. The challenges chill whistle-blowing and thereby undermine public access to information and the democratic role of the media. In turn this jeopardizes the sustainability of quality journalism.

The present research provides a comprehensive review of developments that can impact on the legal frameworks that support protection of journalistic sources. Interviews, panel discussions, thematic studies and a review panel ensured the input of legal and media experts, journalists and scholars. The study provides recommendations for the future of journalistic source protection.

United Nations
Educational, Scientific and
Cultural Organization

Communication and
Information Sector

9 789231 002199