The Privacy Surgeon

A Crisis of Accountability

A global analysis of the impact of the Snowden revelations

Compiled and edited by Simon Davies

June 2014

Published in association with

Institute for Information Law
Faculty of Law - University of Amsterdam

LSTS
Law, Science, Technology & Society Studies
Vrije Universiteit Brussel
Belgium

www.privacysurgeon.org

@PrivacySurgeon

Contents

Acknowledgments

This report was made possible through the huge support and excellent contributions from the following people, to whom we extend our gratitude:

Steve Anderson (Canada - OpenMedia.org), Carolina Botero (Colombia), Bruna Castanheira (Brazil), Gemma Galdon Clavell (Spain), Nighat Dad (Pakistan), Hauke Gierow (Germany), David Green (Electronic Frontier Foundation, US), Lauri Hirvonen (Finland, Electronic Frontier Finland), Tamir Israel (Canada), Lorena Jaume-PalasÌ (Germany), Otso Kassinen (Finland, Electronic Frontier Finland), Ephraim Percy Kenyanito (Kenya, Access Now),

Melih Kirlidog (Turkey), Monserrat Laguna (Mexico), Cedric Laurant (Mexico), Raegan MacDonald (EU, Access Now), TJ McIntyre (Ireland), Joe McNamee (EU, European Digital Rights – EDRi), Peter Micek (EU), Jenny Ng (Australia), Kurt Westh Nielsen (Denmark), Ville Oksanen (Finland, Electronic Frontier Finland), Christopher Parsons (Canada), Shaikh Rafia (Pakistan), John Razen (Brazil), Gabriella Razzano (South Africa), Mike Rispoli (Privacy International, London),

Paulo Rená (Brazil), Katitza Rodriguez (Electronic Frontier Foundation, US), Gideon Rop (Kenya), Pilar Saenz (Colombia), Amie Stepanovich (US), Katarzyna Szymielewicz (Poland), Jerome Thorel (France), Amalia Toledo (Colombia, Karisma Foundation), Niklas Vainio (Finland, Electronic Frontier Finland), Micheal Vonn (Canada), Rejo Zenger (Netherlands, Bits of Freedom).

Thanks also to the many other civil society organizations who provided advice and networking for this project.

A special thank you to Zarte Siempre, who assisted in the editing and proofing process and to Katitza Rodriguez of the Electronic Frontier Foundation (EFF) for such constant support throughout the project.

Our gratitude also goes to the *Institute of Information Law* of the *University of Amsterdam* and *Law, Science, Technology & Social Studies* (LSTS at the *Vrie Universiteit of Brussels* for their support.

The editor takes sole responsibility for any inconsistencies or misunderstanding in the introduction and analysis of this report.

About the publishing team

This report was conceived and published by the *Privacy Surgeon* (www.privacysurgeon.org) a popular independent commentary and analysis site operated by veteran privacy specialist Simon Davies. Publication is in association with both *the Institute of Information Law* of the *University of Amsterdam* and *Law, Science, Technology & Social Studies* (LSTS at the *Vrie Universiteit of Brussels*.

Simon Davies is widely acknowledged as one of the most experienced and influential privacy experts in the world, and is one of the pioneers of the international privacy arena. He is currently Associate Director with LSE Enterprise (London School of Economics) http://www.lse.ac.uk/businessAndConsultancy/LSEEnterprise/who.aspx and is also a visiting researcher with both *IViR* at the *University of Amsterdam* and LSTS at the *Vrie Universiteit of Brussels,* each of which hosted him during the gestation of this report.

The *Privacy Surgeon* has borne all costs and takes all liability associated with this report.

Executive summary

- The Snowden disclosures have triggered a noticeable shift in thinking across the world toward increased awareness of the importance of accountability, transparency and the rule of law with regard to both the activities of security agencies and the value of privacy. This shift - in many parts of the world - has empowered civil society, created a resurgence of interest in legal protections and sensitised media to key issues that have hitherto escaped public scrutiny at any substantial level.

- This shift notwithstanding, the overwhelming majority of countries assessed in this report have not responded in any tangible, measurable way to the Snowden disclosures that began in June 2013. While there has been a notable volume of "activity" in the form of diplomatic representations, parliamentary inquiries, media coverage, campaign strategies, draft legislation and industry initiatives, there has – at the global level – been an insignificant number of tangible reforms adopted to address the concerns raised by the Snowden disclosures. Two thirds of legal professionals and technology experts from 29 countries surveyed for this study reported that they could recall no tangible measure taken by government.

- While obfuscation and denial were reported across most governments, the UK in particular – as America's principle operational and diplomatic security partner – was singled out because of its almost total disregard for any of the issues raised by the Snowden disclosures.

- The operational relationship between security services, law enforcement agencies and global police organisations such as INTERPOL remains largely unknown and – in terms of data policy – continues to be largely unaccountable. While important new information has been made public about how security agencies collect and exchange data within their own security community, almost nothing is known about the use of that information or the extent to which it is passed to law enforcement agencies.

- The small number of reforms that have been adopted by governments (most notably the US) appear to create no meaningful protections for personal data at the global level. While, for example, President Obama declared an interest in providing some protections for non-US persons, the protections themselves were marginal at best, and have so far failed to materialise. Indeed the available evidence indicates that the US administration has engaged in a global campaign to neutralise attempts by some governments to create reform of international security relationships.

- Despite a perception that the Snowden disclosures have became a global news story, reports from the majority of non-US nations indicate that media coverage in many countries has been minimal or non-existent. Concern was expressed that the story was “owned” as a proprietary package by the Anglo-American press and was of little direct relevance to most parts of the world. This perception only shifted at the local level when such countries as Pakistan and Mexico were specifically cited in leaked documents.

- Possibly in part because of the predominant US focus in reporting, media coverage of the relevant issues has declined globally to less than two percent of the initial traffic of a year ago - and continues to diminish. As a consequence, public concern about the issues raised by the disclosures has – at best – reached a plateau. This drop-off is particularly steep in non-US and non-English language media.

- A significant number of corporations have responded to the disclosures by introducing a range of accountability and security measures (transparency reports, end-to-end encryption etc). Nonetheless, while acknowledging that these reforms are “a promising start” nearly sixty percent of legal and IT professionals surveyed for this report believe that they do not go far enough, with more than a third of respondents reporting that they felt the measures were “little more than window dressing” or are of “little value” outside the US.

- Civil society and the tech community have not adequately adapted to the challenges raised by the Snowden revelations. For example, the interface and the communications between policy reform (e.g. efforts to create greater accountability measures, privacy regulations) and technical privacy solutions (e.g. designing stronger embedded security) is worryingly inconsistent and patchy. Few channels of communication and information exchange exist between these disparate communities.

Introduction and background

Anyone following the US and English-language media in the wake of the Snowden revelations might be forgiven for believing that the disclosures have created a vast impact on the world's security services. The US, in particular, has engaged in a high-profile national debate of sufficient scale to bring some of the US-based intelligence entities to the brink of greater accountability. Despite there being little in the way of tangible benefit for non-US persons, the US developments have created some important advances in security accountability.

Nonetheless, while being the most widely reported of all the elements of Snowden's legacy, the US developments do not in any way represent the international situation. To understand the more common response by governments, one need look no further than the United Kingdom - America's principle operational and diplomatic security partner - which has failed to engage the relevant issues in any meaningful way.

Indeed the intransigence of UK authorities reached such heights that in February 2014 – eight months after the first wave of disclosures by Snowden – the UK Parliament was forced to take the almost unprecedented step of issuing a formal summons to the security services watchdog, Sir Mark Waller, who had repeatedly refused to appear before the Parliament's investigating committee.[1]

The Waller episode appears symptomatic of the UK government's post-Snowden mindset. The following month, the *Privacy Surgeon* lodged a formal plea with the Attorney General to use his prerogative to request a police investigation of UK spy agency GCHQ over apparent criminal violations of communications interception law. The lengthy request, written in collaboration with legal specialists, had no effect. Indeed the Attorney General's office has not even responded to the correspondence.[2]

Government and oversight authorities in many countries have behaved in a similar vein, often with little or no international media coverage.

By the beginning of 2014 it had become clear to observers and analysts that the global response to the Snowden disclosures was erratic and often unknown. While, for example, Germany, Brazil and the European Parliament were quite active in establishing response mechanisms to address the revelations, the same could not be said of nations in many parts of the world – or indeed, in many parts of Europe.

---

[1] http://www.theguardian.com/uk-news/2014/feb/27/mps-summon-security-services-watchdog-mark-waller-snowden

[2] http://www.privacysurgeon.org/blog/incision/attorney-general-receives-plea-to-refer-gchq-interception-to-uk-police/

This report arose, therefore, from a growing awareness that a more comprehensive assessment of the global response to Snowden was required. This analysis would help inform the global movement that has arisen to bring reform and accountability to security services. One primary aim is to provide media, campaigners, opinion leaders and the public with a reliable source that presents the facts in a comparative format.

There were many questions that needed to be addressed, including:

1. *Outside of the US, have there been any concrete reforms undertaken by governments or other organisations?*

2. *In terms of the activity over the past year, what patterns and common threads, if any, can be deduced?*

3. *From this evidence, what lessons can be learned about how to take the reform agenda forward over the coming years?*

This report is not cerned with opinion or aspiration. It describes concrete, measurable outcomes rather than simple “activity”. This entails not just citing, for example, that an inquiry was conducted or a parliamentary debate held, but whether a tangible measure has been implemented as a result of that activity.

The methodology chosen was to identify a number of trusted experts in selected countries that we believed would be representative of the global landscape. To this end correspondents were secured to present brief reports on Australia, Brazil, Canada, Colombia, France, Ireland, the EU, Netherlands, United States, United Kingdom, Pakistan, Kenya, Germany, Mexico, South Africa, Poland, Finland, Denmark and Spain together with a sector report on the response by industry.

To provide further input to these reports, an online survey was then conducted amongst nearly a hundred academics, legal professionals and IT experts in a further nineteen countries - Uruguay, Belgium, Italy, Serbia, Japan, Romania, India, Israel, Singapore, Portugal, Turkey, Greece, Burundi, the Philippines, Austria, Sweden, Slovenia, Bulgaria and Malaysia. These respondents – like the country correspondents – were asked to provide information on measurable reforms in their respective countries, together with their own assessment of the impact of the Snowden disclosures on public and government perspectives.

In summary, this report is not intended to be a legal analysis, nor does it attempt to analyse policy positions. Its role is to provide information on constructive developments across the world and to discuss possible measures to accelerate the pace of those developments.

Analysis

Global security relationships are complex, embedded and often inscrutable. They have evolved over many decades, bolstered by secretive arrangements and an operational framework that is – at best – deeply opaque.

However, since June 2013, much has been learned about the workings of the security ecosystem. A critically important sliver of that arena has been opened up, in particular the data collection and analysis operations conducted by the US National Security Agency and its close allies.

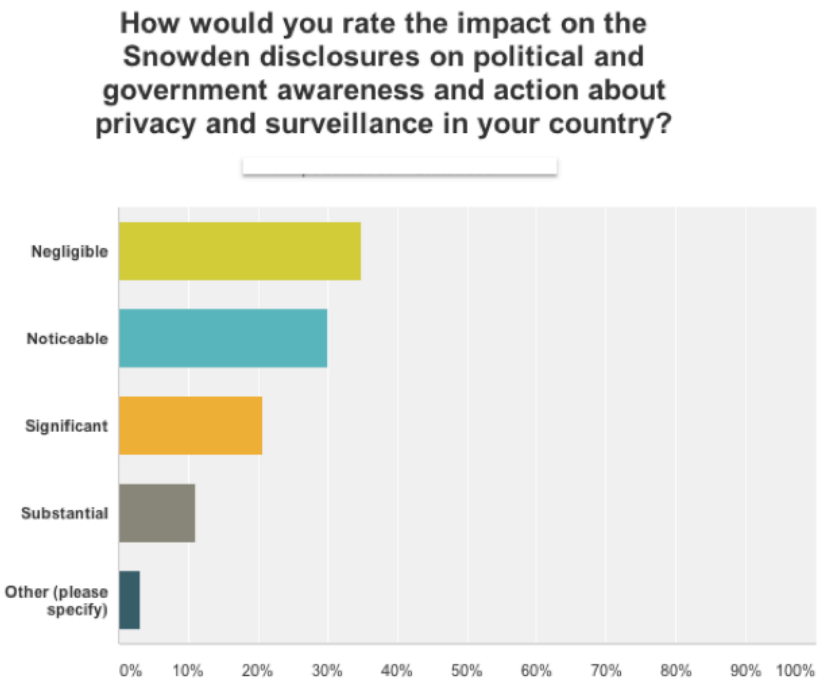
For those who are not specialists in this field, one of the best evidence-based primers on the subject was recently published[3] by the Electronic Frontier Foundation (EFF), outlining 65 key facts about the National Security Agency (NSA) that until 2013 were not known. This document is an effective starting point for anyone interested in the subject.

The EFF summary does, however, focus primarily on US-based security activities. While these are of crucial to global privacy (or at least, the intrusion into privacy), there is much still to be discovered, both about the enabling international arrangements and the activities of individual non-US national security services.

It is equally true that the operational relationship between security services, law enforcement agencies and global police organisations such as INTERPOL remains largely unknown and – in terms of data policy – continues to be largely unaccountable. While important new information has been made public about how security agencies collect and exchange data within their own security community, relatively little is known about the use of that information or the extent to which it is passed to law enforcement agencies. That is, while the public now has a better understanding of how personal information is collected by agencies (particularly the NSA), relatively little is known about how that data is used beyond the point of collection. The accountability gap in the security realm is thus even greater than many inquiries and analysts have suggested.

Despite these shortcomings, the evidence presented in this report indicates that the Snowden disclosures have resulted in an overall change in public perception and a spike in political sensitivity around such issues as accountability of security services. While this has not so far translated universally into concrete reforms, the shift is an indication that an additional foundation stone may have been laid in some countries that will enable tangible reform.

[3] https://www.eff.org/deeplinks/2014/06/65-65-things-we-know-about-nsa-surveillance-we-didnt-know-year-ago



Around thirty percent of respondents to the online survey believed there has been a "substantial" or "significant" impact on government awareness.

Reform, however, cannot be measured merely through the actions of government. Industry has to some extent responded in a proactive manner to institute a range of measures to improve privacy and security. At the time of publication of this report Vodafone, one of the world's biggest mobile providers, is on the point of disclosing basic details of the "backdoor" access that security agencies have to its networks, allowing security bodies to listen in to any phone channel they choose.

In its report on the disclosure, the Guardian[4] commented:

> *The company has broken its silence on government surveillance in order to push back against the increasingly widespread use of phone and broadband networks to spy on citizens, and will publish its first Law Enforcement Disclosure Report on Friday . At 40,000 words, it is the most comprehensive survey yet of how governments monitor the conversations and whereabouts of their people.*

Such detailed transparency was unheard-of before the Snowden era. Clearly, there has been a significant shift in view amongst some corporations in response to what is perceived as an abuse of surveillance facilities by security

[4] http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

and law enforcement. Australian authorities, for example, made an extraordinary 685,757 requests for communications metadata in 2013, almost three times the number of requests per head of population made by the UK, and more than a hundred-fold greater than Germany.[5]

As the industry report below in this report observes, the move to transparency in the relations between corporations and government has been significant, but was not triggered exclusively by the Snowden disclosures. Indeed the transparency trend has been in progress since at least 2009. Of greater importance perhaps is the trend to the endemic strengthening of communications security. This development – pursued by a number of companies – goes beyond mere transparency and moves toward creating at least the beginning of a more privacy-secure communications ecosystem. Whether this results in an escalation of the technology arms race is yet to be seen.

Critics are right to point out that the mere disclosure of information about the extent of systemic intrusion by security agencies is not, in itself, a sufficient response. Nonetheless, corporations have started to move, by degrees, to changing the dialogue around surveillance, particularly with regard to legal and ethical principles. This shift to some extent reflects the commercial market for privacy that has been evolving for some years.

This trend was eloquently expressed by Microsoft's General Counsel Brad Smith on the first anniversary of the Snowden debut. Arguing that the US needs to respect international sovereign protections[6], Smith argued:

> *These concerns have real implications for cloud adoption. After all, people won't use technology they don't trust. We need to strike a better balance between privacy and national security to restore trust and uphold our fundamental liberties.*

Civil Society has also responded with measures that will help build stronger constituencies and coalitions including such initiatives as the *Thirteen Principles*[7] and the *Don't Spy on Us* coalition.[8]

The bigger picture

While this report is centred on reviewing measurable reforms, the authors understand that the one-year period being assessed is in many respects too short a time frame to gauge the true impact of the Snowden influence.

---

[5] http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

[6] http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/06/04/unfinished-business-on-government-surveillance-reform.aspx

[7] https://en.necessaryandproportionate.org/text

[8] https://www.dontspyonus.org.uk/org

Nevertheless, the period may be considered in terms of trends, i.e. whether the pace of reform has accelerated, slowed or reached a plateau.

In some respects - and despite the encouraging trends described above - the outcome for reform is not entirely positive. More than half the countries surveyed for this project reported that there has been little media or political activity as a result of the disclosures. Of the remainder, around a half identified tangible reforms that had been pursued, and most of those correspondents expressed concern that reform activity had slowed in recent months. Overall, around one sixteenth of countries are on target for even the most marginal reform of their security services.

Around seventypercent of respondents to the online survey could not recall any positive action by government.

This situation should not diminish the significance of the broader trend of public awareness and political activity. There have been several substantial outcomes, including action by the UN, the European Parliament and the White House. A noticeable geo-political shift has occurred, though this dynamic largely excludes Africa and Asia.

At this early stage it is difficult to determine the extent to which the disclosures have influenced other social and political developments. In Turkey, for example, the Snowden revelations came during the peak of the Gezi uprising. Since it became obvious that there is almost no privacy in social media (which was heavily and effectively used in the events), the "occupiers" were

concerned about how the collaboration between large ICT companies and the NSA might extend to the Turkish government. This resulted in an awareness of Internet privacy issues and some web sites that provide advise on privacy issues emerged.[9]

Many of the country assessments in this report highlight the significance of the shift in thinking over privacy and security issues, emphasising the real potential for future reform. Spain, for example, observed:

> *There are signs that a debate has been sparked, at least in specific milieus and in relation to cybersecurity, social media and privacy concerns. And while the media and political passivity is an immediate challenge, general privacy concerns have managed to become the standard in technology reporting and policy. In this evolving context, every new revelation on the use and abuse of surveillance powers is contributing to strengthening the need for a true public debate on the possibilities and risks of the surveillance society.*

Colombia also emphasised the broader influence of this change of perspective:

> *If Snowden's revelations have had some influence in Colombia it was to highlight the fact that intelligence decisions cannot be based solely on State security rationale. To some extent, these revelations have served to demonstrate that there are limits to state surveillance activities. It has also shown that there is a need to guarantee citizens' rights, as well as to establish civil society oversight mechanisms. Yet, it will take some time to translate this recognition to the domestic reality.*

while Canada reinforced the interactive elements of the reform process:

> *In conclusion, the media and Parliament's attention to signals intelligence has increased significantly, and these efforts have dovetailed with ongoing concerns over the scope and nature of privacy-invasive activities by domestic state agencies.*

The disappointing media coverage in many parts of the world could be a result of either under-management or over-management of the Snowden disclosures. Despite a perception that the Snowden disclosures have became a global news story, reports from the majority of non-US nations indicate that media coverage in many countries has been minimal or non-existent. Concern was expressed that the story was "owned" as a proprietary package by the Anglo-American press and was of little direct relevance to most parts of the world. This perception only shifted at the local level when such countries as Pakistan and Mexico were specifically cited in leaked documents.

Possible shortcomings in the Guardian's handling of the Snowden episode

[9] One successful example is Capul.tv. http://capul.tv

could be explained by a business motivation to create roots in a more lucrative global market, particularly the US.[10] Nonetheless – as the experience of such countries as Brazil has demonstrated in this report – the newspaper's handling of the story has in some respects been highly effective, even if over-protective of the data.

Future action

One challenge for the years ahead will be to extend this issue beyond the Trans-Atlantic domain and into a truly global context. This requires more than mere media attention and goes to the question of innovative, integrated strategy that binds all elements of the reform community. There are several key initiatives globally that will strengthen and streamline citizen-led initiatives to pressure governments and corporations to create better defences for privacy over the next few years.

The data in this report may help indicate some other important pathways to future action for reform. One of the most significant of these relates to interactivity between different strands of the reform community. Civil society and the tech community have not adequately adapted to the challenges raised by the Snowden revelations. For example, the interface and the communications between policy reform (e.g. efforts to create greater accountability measures, privacy regulations) and technical privacy solutions (e.g. designing stronger embedded security) are worryingly inconsistent and patchy. Few channels of communication and information exchange exist between these disparate communities. There was also a sense that reform strategy needed to become more effective – even aggressive – if further progress was to be made in the foreseeable future.

One response to these outcomes has been an informal agreement among several NGO's to participate in a collaborative process over the summer called "Code Red". This initiative will aim to build working interfaces that do not currently exist, and seek accelerated resources and funding for cutting-edge technical responses, legal challenges, direct action and innovative policy reform.

A further announcement about this initiative will be made in early September.

[10] http://thenextweb.com/media/2013/07/30/the-guardian-newspaper-moves-its-uk-us-and-australian-websites-to-a-new-com-domain-today/

Country and sector reports

Contributor biographies are set out in the final section of the report

Australia

Snowden's disclosures affect Australia, as that country is one of the 'Five-Eyes' alliance of intelligence partners. Australia's electronic intelligence agency is called the *Australian Signals Directorate* (ASD), previously known as the *Defence Signals Directorate*. The disclosures showed that the Australian intelligence agency surveillance programs targeted Indonesia, East Timor, Malaysia and the Philippines, with information shared with the US. They also show that Australia offered to share information on ordinary Australians with the Five-Eyes partners.[11]

This created concern amongst Australian legal, digital rights and civil liberties communities. Geoffrey Robertson QC argues that ASD breached the law in offering detailed information on Australian citizens to its foreign partners.[12]

Disclosures about Australia's involvement received wide coverage in Australian media. The then Labor government Attorney-General, Mark Dreyfus, received secret briefings on PRISM in March 2013, months before Snowden revealed that information.[13] Australian agencies were reported to have spied on Indonesian president Yudhoyono and his wife.[14] Commercial

---

* David Vaile (co-convenor, Cyberspace Law and Policy Community, UNSW) and Nigel Waters (Australian Privacy Foundation and Privacy International) are thanked for commenting on the draft of this report.

[11] Revealed: Australian spy agency offered to share data about ordinary citizens, The Guardian, http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens

[12] The privacy of ordinary Australians is under serious threat, The Guardian, http://www.theguardian.com/commentisfree/2013/dec/02/privacy-australians-surveillance-metadata

[13] Australia prepared briefing on US global internet spying program PRISM before Snowden revelations, ABC News, http://www.abc.net.au/news/2013-10-08/australia-prepared-briefing-on-prism-spying-program/5004290

[14] Australia spied on Indonesian president Susilo Bambang Yudhoyono, leaked Edward Snowden documents reveal, ABC News, http://www.abc.net.au/news/2013-11-18/australia-spied-on-indonesian-president-leaked-documents-reveal/5098860 ; Edward Snowden

advantage in trade negotiations appears to be the motive for spying on a US law firm representing Indonesian clove and prawn suppliers.[15] Australia monitored phone calls in the Philippines.[16] Furthermore, the Malaysian government, political leaders and defence had been targeted by ASD for years.[17] A leaked map shows four Australian sites involved in US global intelligence collection which are the US-Australian Joint Facility at Pine Gap, the Australian Defence Satellite Communications station near Geraldton (WA), the Shoal Bay Receiving Station near Darwin, and another site near Canberra. [18]

In late June 2013, the Joint Parliamentary Committee on Intelligence and Surveillance (JPCIS) declined to endorse a sketchy AGs proposal, with no legislative draft, for data retention on an increased scale. Snowden's revelations, combined with reluctance by agencies and AGs to offer detail, pushed JPCIS into a rare query for a request for greater legal scope for surveillance.

Greens Senator Ludlam pushed a motion for a Senate review of electronic surveillance, known as the *Senate Select Committee on Electronic Surveillance*. Major parties have refused earlier attempts to establish an inquiry. The motion to re-establish the Joint Standing Committee on Intelligence and Security was refused. On December 2013, the Greens party announced that Senator Ludlam's Senate motion was successful.[19] These developments have led to the inquiry into a comprehensive revision of the Telecommunications (Interception and Access) Act 1979.[20] The review will report in August 2014. However, the Inspector-General rejected any inquiry into allegations that the ASD offered information about Australians to foreign agencies. Ludlam commented on 'The Day We Fight Back', 11 February 2014, that the debate in Australia is subdued compared to the US.[21]

---

documents reveal Indonesian phone networks penetrated by Australian spies, SMH, http://www.smh.com.au/federal-politics/political-news/edward-snowden-documents-reveal-indonesian-phone-networks-penetrated-by-australian-spies-20140216-32tyu.html

[15] Spying by N.S.A. Ally Entangled U.S. Law Firm, NYT, http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html

[16] Australian spies secretly monitor phone calls in the Philippines: Edward Snowden disclosure, SMH, http://www.smh.com.au/technology/technology-news/australian-spies-secretly-monitor-phone-calls-in-the-philippines-edward-snowden-disclosure-20140520-zri6r.html

[17] Edward Snowden documents show Malaysia is an Australia, US intelligence target, SMH, http://www.smh.com.au/world/edward-snowden-documents-show-malaysia-is-an-australia-us-intelligence-target-20140330-zqonc.html

[18] Australia-US spy links exposed by Edward Snowden, The Australian, http://www.theaustralian.com.au/national-affairs/policy/australia-us-spy-links-exposed/story-fn59nm2j-1226676189326#mm-premium

[19] Internet surveillance: today is the day we fight back http://www.theguardian.com/commentisfree/2014/feb/11/day-fight-back-against-internet-surveillance-scott-ludlam

[20] See http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report/index.htm

[21] Internet surveillance: today is the day we fight back

The Australian Law Reform Commission is likely to recommend in June a new tort of serious invasion of privacy, to complement limited protection for personal information provided by the *Privacy Act* 1988 (Cth). The 2014 amendments to the *Privacy Act* strengthened enforcement powers but weakened the Principles, and retain law enforcement and 'authorised by law' exceptions. The tort would enable Australians to litigate for privacy. This is a step forward, but it is unclear if disproportionate surveillance would be covered.

The new conservative government seems unlikely to implement the proposed privacy tort or give the Privacy Commissioner adequate resources. It also seems uninterested in reining in powers or activities of intelligence and law enforcement agencies, or considering risks and harm to individuals, businesses or the public interest from erosion of trust in communications confidentiality, IT security and privacy.

However, Snowden's disclosures have given privacy and surveillance issues a higher profile than ever before and in the longer term may lead to improvements in legal privacy protection. The outcome is by no means certain, with the capacity for inhibiting stronger privacy laws ever present.

Correspondent: Dr Jenny Ng

---

http://www.theguardian.com/commentisfree/2014/feb/11/day-fight-back-against-internet-surveillance-scott-ludlam

Brazil

The Snowden revelations have triggered a significant international political reaction from the Brazilian government. But that happened only after Glenn Greenwald, enabled with Snowden's leaks and living in Rio de Janeiro, started to release information about NSA surveillance over the Brazilian National Oil Company – Petrobrás [1] and the communications of the Brazilian President Dilma Roussef [2].

This breaking news was broadcast in the most popular TV program of the week in the biggest media outlet in the country over a series of Sunday night shows. Such media outreach made Brazilian authorities frame the NSA scandal as an issue of national sovereignty, leading President Dilma to request clarification from the U.S. government. Without any substantive answer even after a call with President Barak Obama himself, she has canceled a visit previously scheduled to the country [3].

In order to collect more information, the Senate has installed a Parliamentary Commission for Inquiry, entitled “CPI da Espionagem”, where ICT companies, Glenn Greenwald and others where invited to testify [4]. The Brazilian Federal Police had also opened an investigation, calling the presidents of Yahoo, Microsoft, Google, Facebook and Apple to testify [5] and even requested to interrogate Edward Snowden.

After postponing her visit to the US, the first international answer by President Dilma was a strong statement at the UN General Assembly [6] in which she stressed that *"in the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy*.” She also highlighted that *“the right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country*” and that *“in the absence of the respect for sovereignty, there is no basis for the relationship among nations."*

Indeed, the notion of sovereignty started to be restated in national debates for legislation. As a declared response to NSA surveillance, the government has proposed changes in the text of *Marco Civil,* the Draft Bill for a Civil Right

Framework for the Internet in Brazil. The most polemic of these mentioned the possibility to oblige some ICT companies to nationalize their data centers. Ultimately, that proposal was dropped from the text, but the final text still stipulates that *"any operation regarding collection, storage, treatment and storage of data or personal communications by ISPs that occurs in Brazilian territory must respect Brazilian legislation and the rights to privacy, protection of personal data and confidentiality of private communications and records.*" The draft bill also had many changes regarding extending the provisions on privacy rights. [7]

After all theses changes were proposed, the President also declared constitutional urgency for Marco Civil. This meant that National Congress would have a fixed term to analyze it, otherwise, the agenda would be blocked and no other draft proposal could be considered. The text received approved during the course of another outcome of the Snowden Revelations, the diplomatic meeting entitled *NetMundial*, hosted in Sao Paulo in April, 23rd and 24th.

Also known as a global *multistakeholder meeting on the future of Internet governance* [8], NetMundial was conceived in the aftermath of the Snowden revelation's to gather different stakeholders from the international community to discuss the elaboration of universal principles for Internet governance and a proposal for a roadmap for future development of this ecosystem. Nevertheless, even though mass surveillance practices where the main issue that sparkled the idea of such debate, the final text, entitled the *NetMundial Multistakeholder Statement* [9], has just one paragraph about the topic:

> *"Mass and arbitrary surveillance undermines trust in the Internet and trust in the Internet governance ecosystem. Collection and processing of personal data by state and non-state actors should be conducted in accordance with international human rights law. More dialogue is needed on this topic at the international level using forums like the Human Rights Council and IGF aiming to develop a common understanding on all the related aspects."*

Even though negotiated outside the UN system, in a context in which raw consensus was acceptable, the text doesn't go beyond the statement in the Resolution entitled *"Right to Privacy in the Digital Age*", which was proposed by Brazil and Germany and approved by consensus in the UNGA [10].

It was also in April 2014 that the final report from "*CPI da Espionagem*" was released [11]. Over more then 300 pages this document attests the country's fragility in face of international mass surveillance of electronic communications and suggests measures for improving national cybersecurity, including a draft bill regarding access to Brazilian users' data by foreign authorities. [12] The approved text will be forwarded to several public agencies. Even though President Dilma has reaffirmed in her speech at UNGA that there is a need to *"create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage and*

attacks against systems and infrastructure", it seams that the path is heading in the other direction.

Brazil was not been identified in the NSA scandal as an agent of surveillance, only as a country under surveillance. As such, the focus of reactions to Snowden's revelations in the country were mostly on the USA. No real attention has been given to the involvement of the other Five Eyes countries. Nonetheless, since the protests of June, 2013 - and now in preparations for the World Cup - national surveillance by the Brazilian State has also been a increasing concern. [13]

Snowden in Brazil?

In August, 2013, David Miranda, the Brazilian partner of Glenn Greenwald who lives in Rio, was detained for nine hours by Scotland Yard officers at Heathrow Airport in London, under the justification of counter-terrorism. [14] The detention was highly criticized by Brazilian media and gave Miranda some visibility in media outlets. In the aftermath of his detention, Miranda started an online campaign [15] for granting political asylum to Snowden in Brazil, currently with more then one million signatures.

In December, 2013, the newspaper *"Folha de S. Paulo*" published an *"Open Letter to the People of Brazil"* [16], in which Snowden himself said the White House would continue interfering in his *"ability to speak*" until he is granted permanent asylum in some country, suggesting that in Brazil he could assist the government investigations regarding espionage by Washington. During the "CPI da Espionagem" several congressman have expressed sympathy for grating Snowden asylum in the country.

Recently, in May, 2014, Snowden gave an interview to *Fantástico*, the most viewed program on Sunday open TV, reaffirming once again that if Brazil grants him asylum, he would come. [17] Nevertheless, though confirming the receipt of a formal request for asylum from Snowden at the Brazilian Embassy in Moscow, the Brazilian government has never responded to it, and representatives from the Ministry of Foreing Affairs have reinforced that there is no intention to deal with such a request. [18]

---

[1] Petrobras foi alvo de espionagem de agência dos EUA, aponta documento, in http://g1.globo.com/politica/noticia/2013/09/petrobras-foi-alvo-de-espionagem-de-agencia-dos-eua-aponta-documento.html
[2] Documentos da NSA apontam Dilma Rousseff como alvo de espionagem, in http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html
[3] Dilma cancela viagem aos EUA, in http://politica.estadao.com.br/noticias/geral,dilma-cancela-viagem-aos-eua,1075730
[4] CPI da Espionagem, in

http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=&com=1682
[5] PF quer ouvir as empresas americanas sobre espionagem - notícias em Mundo", in http://g1.globo.com/mundo/noticia/2013/10/pf-quer-ouvir-empresas-americanas-sobre-espionagem.html
[6] Dilma speech at UNGA, in http://gadebate.un.org/68/brazil
[7] http://antivigilancia.tk/wiki/boletim_antivigilancia/9
[8] http://netmundial.br/about/
[9] http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
[10] http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
[11] Relatório Final CPI Espionagem, in http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1
[12] Brasil está muito exposto à espionagem, aponta relatório, in http://www12.senado.gov.br/noticias/materias/2014/04/09/brasil-esta-muito-exposto-a-espionagem-aponta-relatorio
[13] Motherboard - The FBI Is Training Brazil's New Tech-Savvy Riot Police", in http://motherboard.vice.com/read/the-fbi-is-trainingbrazils-new-tech-savvy-riot-police / http://rt.com/news/brazil2014-us-military-robots-501/
[14] http://www1.folha.uol.com.br/mundo/2014/02/1414398-detencao-de-david-miranda-em-aeroporto-de-londres-foi-legal-diz-justica-britanica.shtml
[15] https://secure.avaaz.org/po/petition/Asilo_ja_para_o_Inimigo_Publico_Numero_1_dos_EUA/
[16] "Leia íntegra da carta de Snowden ao Brasil - 17/12/2013 - Mundo - Folha de S.Paulo", in http://www1.folha.uol.com.br/mundo/2013/12/1386291-leia-integra-da-carta-de-snowden-ao-brasil.shtml
[17] http://g1.globo.com/fantastico/noticia/2014/06/se-o-brasil-me-oferecer-asilo-aceito-diz-edward-snowden.html
[18] http://noticias.uol.com.br/internacional/ultimas-noticias/2013/12/18/eu-me-dou-o-direito-de-nao-me-manifestar-sobre-snowden-diz-dilma.htm
http://gizmodo.uol.com.br/brasil-nega-asilo-edward-snowden/

Correspondents: Paulo Rená, Joana Varon, John Razen, Bruna Castanheira

Canada

Snowden's revelations have implicated Canada's foreign intelligence signals agency -- *the Communications Security Establishment Canada* (CSEC) -- in expansive domestic and foreign surveillance initiatives. To date, however, the Snowden effect has led to few tangible or significant reforms designed to remedy problematic surveillance practices exposed by the Snowden revelations. The most significant responses have included civil society and media commentary, some parliamentary action in the form of criticism, fact-finding activities and reform efforts, and early judicial and quasi-judicial interventions. These collective efforts have dovetailed with (and enhanced) previous efforts at reform of Canada's foreign intelligence and domestic surveillance regime. While the net result has led to a greater understanding of CSEC's activities and objectives, there has been minimal concrete movement towards reform aside from some early judicial proceedings.

Canadian media have received and published several Snowden documents implicating CSEC. These publications have been supplemented by domestic investigative media efforts. CSEC has been controversially implicated in surveillance of the Brazilian Ministry which grants resource exploitation contracts, [1] in undermining of international security standards, [2] in aiding five eyes partners to spy on political allies during G8 and G20 meetings, [3] and in using CSEC's metadata reserves to map individual movements and infrastructure in Canada by monitoring public wifi networks. [4] Canadian media has also documented the dramatic growth in CSEC's budget in recent years, as well as its close financial links to foreign agencies such as the U.S. National Security Agency. [5] General concern over CSEC has led to calls for reform of Canada's foreign intelligence surveillance apparatus by a number of major Canadian newspapers. [6] It should be noted that while the media response has been significant by historical standards, it has largely remained driven by Canadian-specific revelations.

In response to the Snowden disclosures, Canadian civil society and academics have worked to raise awareness of state surveillance. This has included education campaigns and online actions. Notably, the *Protect Our Privacy Coalition* -- comprised of over 50 major organizations and two-dozen leading academics -- launched an online action calling on Members of Parliament to rein in CSEC's more intrusive activities as part of an internatoinal day of action. [7] Academics have convened workshops and high profile debates, [8] and publicly explained the significance of state surveillance online and through media. One workshop launched

a book on surveillance in Canada [9] and generated the Ottawa Statement on Mass Surveillance. [10] Additional efforts from researchers at the University of Toronto have tried to ascertain how long Internet service providers collect, retain, and handle subscriber data, as well as data routing practices, [11] and to pressure telecommunications companies into improving their transparency regarding disclosure of customer data to state agencies. [12] These efforts have only recently begun yielding some responses from private telecommunications companies in the form of transparency reports, [13] but no commitment to change from the federal government or from CSEC.

Canada's legislative bodies have also been active. The Senate Standing Committee on National Security and Defence is studying CSEC's activities [14] and may produce a report with recommendations for reform. Opposition parties in Canada's primary legislative body -- the House of Commons -- have called for an emergency debate on CSEC's surveillance activities [15] and for the government to commit to transparency and reform of CSEC. [16] Opposition MP Charmaine Borg attempted to force the disclosure of statistics concerning the scope of government's agencies' surveillance efforts (including CSEC's) and met with limited response from domestic agencies and none from CSEC. [17] Finally, two bills have been introduced by individual MPs to enhance oversight of CSEC's activities; [18] unfortunately, neither has the government's support nor do they include amendments to CSEC's substantive legal or operational framework.

The most promising developments in Canada have arisen from judicial and quasi-judicial initiatives. First, Justice Mosley of the Federal Court reconsidered, on his own initiative, a surveillance authorization decision he had issued in 2009. The authorization let the Canadian Security and Intelligence Service intercept, with CSEC's assistance, the communications of two Canadians travelling abroad as long as the communications transited through Canada. [19] In late 2013, Justice Mosley issued a strong rebuke to CSEC and CSIS for strategically omitting critical information in their 2009 warrant application relating to CSEC's use of its significant and expansive Five Eyes resources in support of the authorized interceptions. [20] As a result of this decision (which will be appealed) CSEC cannot use its Five Eyes resources when assisting domestic agencies with their surveillance activities.

Additionally, the British Columbia Civil Liberties Association (BCCLA) has brought a constitutional challenge to key aspects of the legal and operational framework that governs CSEC. The suit alleges that CSEC's current operations and limited oversight infringe sections 8 and 2(b) of the Canadian Charter of Rights and Freedoms which enshrine the right to be free of unreasonable search and seizure and the freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication. [21] The BCCLA has also filed a proposed national class action lawsuit on behalf of Canadians whose private communications and metadata have been collected by CSEC in a manner that violates the Charter. [22] The Canadian Civil Liberties Association (CCLA) has also launched a lawsuit, challenging the constitutionality of key provisions of PIPEDA, Canada's federal data protection statute, which prevent private companies such as ISPs from effectively notifying customers when their data has been handed over to state agencies such as CSEC for investigative purposes. [23] Finally, the federal privacy commissioner also

released information concerning the regularity at which telecommunications companies were asked for data by government agencies in 2011, though without specificity concerning how often these requests were made by, or on the behalf of, CSEC. [24]

In conclusion, the media and Parliament's attention to signals intelligence has increased significantly, and these efforts have dovetailed with ongoing concerns over the scope and nature of privacy-invasive activities by domestic state agencies. However, this attention has yet to culminate in any concrete outcomes, as the federal government has so far refused to respond to public criticism of CSEC's activities. The most promising actions to date have manifested in the courts, though these actions remain in a nascent state.

ENDNOTES:

[1] Colin Freeze and Stephanie Nolen. 2013. "Charges that Canada spied on Brazil unveil CSEC's inner workings," The Globe and Mail, October 7, 2013, http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/; Colin Freeze, "Read a CSEC Document that was first acquired by Edward Snowden," The Globe and Mail, November 30, 2013, http://www.theglobeandmail.com/news/politics/read-a-csec-document-on-brazil-that-was-first-acquired-by-edward-snowden/article15699941/; for the most publicly detailed analysis of the program see: Anonymous, "OLYMPIA: How Canada's CSEC maps phone and internet connections," Top Level Communications, May 14, 2014, http://electrospaces.blogspot.ca/2014/03/olympia-how-canadas-csec-maps-phone-and.html.

[2] "Government Announces Steps to Restore Confidence on Encryption Standards," http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/; Michael Geist, "Canada Facilitated NSA's Effort to Weaken Encryption Standards", September 11, 2013, MichaelGeist.ca, http://www.michaelgeist.ca/content/view/6951/196/; Omar El Akkad, "The Strange Connection Between the NSA and an Ontario Tech Firm", January 20, 2014, Globe and Mail, http://www.theglobeandmail.com/technology/business-technology/the-strange-connection-between-the-nsa-and-an-ontario-tech-firm/article16402341/.

[3] "NSA document raises questions about Canada in G8 spying," http://www.cbc.ca/news/politics/nsa-document-raises-questions-about-canada-in-g8-spying-1.2447398; "NSA Briefing Note on G8/G20 Summits," http://www.cbc.ca/news2/pdf/summit-doc.pdf.

[4] Greg Weston, Glen Greenwald & R> Gallagher, "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents," January 31, 2014, CBC News, http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881; "IP Profiling Analytics & Mission Impacts (Snowden slides)," http://www.cbc.ca/news2/pdf/airports_redacted.pdf; for analyses of the slides see: Tope Level Telecommunications, "Did CSEC really track Canadian airport travellers", February 4, 2014, http://electrospaces.blogspot.ca/2014/02/did-csec-really-tracked-canadian.html; and

R. Deibert, “Now we know Ottawa can snoop on any Canadian. What are we going to do?” January 31, 2014, http://www.theglobeandmail.com/globe-debate/now-we-know-ottawa-can-snoop-on-any-canadian-what-are-we-going-to-do/article16625310/.

[5] Colin Freeze, “How CSEC Became an Electronic Spying Giant”, November 30, 2013, Globe and Mail, http://www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694/; Ian MacLeod, “Canadian Spies Receive U.S. Money for Research and Surveillance, Book Says”, December 5, 2014, Ottawa Citizen, http://www.ottawacitizen.com/Canadian+spies+receive+money+research+surveillance+book+says/9835864/story.html.

[6] “Globe Editorial: Hey CSEC, stop spying on me,” April 3, 2014, http://www.theglobeandmail.com/globe-debate/editorials/dont-spy-on-me-csec/article17781948/; “Globe Editorial: Canada needs a royal commission on spying and privacy of Canadians,”, May 21, 2014, http://www.theglobeandmail.com/globe-debate/editorials/we-need-a-royal-commission-on-spying/article18786038/; “Canada’s oversight of spy agencies falls short,” http://www.thestar.com/opinion/editorials/2014/02/02/canadas_oversight_of_spy_agencies_falls_short_editorial.html; “National Post Editorial Board: Our spies need oversight,” October 11, 2013, http://fullcomment.nationalpost.com/2013/10/11/national-post-editorial-board-our-spies-need-oversight/.

[7] See: the “Protect Our Privacy Coalition", https://openmedia.ca/ourprivacy. Major actions by participants include: “Call on your MP to stand against costly online spying,” https://openmedia.ca/stand; “World Speaks Out Against Mass Surveillance in Global Day of Online Protest: Day We Fight Back,” https://www.cippic.ca/en/news/day_we_fight_back; L. Tribe, “The day we fight back: Stand up against mass surveillance,” February 11, 2014, https://cjfe.org/blog/day-we-fight-back-stand-against-mass-surveillance; PEN Canada, “The Day We Fight Back: Calling for an End to Mass Surveillance,” February 11, 2014, http://pencanada.ca/campaigns/day-we-fight-back-pen-canada-calls-end-mass-surveillance/. Other major online actions have included: “Tell Harper: Defend Online Privacy,” https://openmedia.ca/defendprivacy; “Call on your MP to stand against costly online spying,” https://openmedia.ca/stand; “Stand with the BCCLA,” https://openmedia.ca/csec; “Protect Our Privacy,” https://openmedia.ca/ourprivacy.

[8] Examples include: Ontario Information & Privacy Commissioner, “Big Surveillance Demands Big Privacy - Enter Privacy-Protective Surveillance”, Toronto, http://www.realprivacy.ca/index.php/international-privacy-day-symposium/; “The Politics of Surveillance: Advancing Democracy in a Surveillance Society,” May 8-10 at University of Ottawa; “Munk Debates on State Surveillance,” May 2, 2014; RightsWatch Conference 2013, September 20-21, 2013, Toronto, http://ccla.org/events/rightswatch-2013/#Program; “CSEC Panel,” April 8, 2014 at Queen’s University; “Intelligence and National Security Panel,” March 21, 2014 at University of Toronto; “Privacy at Risk? The NSA and CSEC, its Canadian Surveillance Partner,” March 12, 2014 at University of Toronto; “Who is Watching the

Watchers? A Panel of Canadian Privacy and Surveillance in the Post-Snowden Era", October 16, 2013, University of Ottawa, Centre for Law, Technology & Society.

[9] "Transparent Lives: Surveillance in Canada," http://www.aupress.ca/index.php/books/120237.

[10] "The Ottawa Statement on Mass Surveillance," http://www.digitallymediatedsurveillance.ca/the-ottawa-statement/.

[11] "Towards Transparency in Canadian Telecommunications," https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/; "The Murky State of Canadian Telecommunications Surveillance," https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/; "IXMaps - See where your packets go," http://ixmaps.ca/.

[12] "Data Privacy Transparency of Canadian Internet Service Providers," http://ixmaps.ca/transparency.php; "Responding to the Crisis in Canadian Telecommunications," https://citizenlab.org/2014/05/responding-crisis-canadian-telecommunications/.

[13] C. Freeze, C. Dobby & J. Wingrove, "TekSavvy, Rogers Break Silence Over Government Requests for Data", June 5, 2014, Globe and Mail, http://www.theglobeandmail.com/technology/tech-news/teksavvy-opens-books-on-government-data-requests/article18999107/. M. Geist, "Rogers' Shocking Admission: It Does Not Track Disclosures of Subscriber Information to Authorities", June 6, 2014, http://www.michaelgeist.ca/content/view/7151/125/

[14] Proceedings of the Senate Standing Committee on National Security and Defence, Canada's National Security and Defence Policies, Practices, Circumstances and Capabilities, February 3, 2014, 62 Elizabeth II, 41st Parliament, 2nd Session, Issue 2, http://www.parl.gc.ca/content/sen/committee/412/SECD/pdf/02issue.pdf.

[15] Charmaine Borg, Terrebonne-Blainville, QC, "Charmaine Borg on Request for Emergency Debate", excerpts from: House of Commons Debates, June 13, 2013, 62 Elizabeth II, 41st Parliament, 2nd Session, http://openparliament.ca/debates/2013/6/13/charmaine-borg-1/only/.

[16] Debates of the Senate, October 24, 2013, 62 Elizabeth II, 41st Parliament, 2nd Session, Volume 149, Issue 5, http://www.parl.gc.ca/Content/Sen/Chamber/412/Debates/005db_2013-10-24-e.htm#35.

[17] Christopher Parsons, "Mapping the Canadian Government's Telecommunications Surveillance", March 27, 2014, Citizen Lab, https://citizenlab.org/2014/03/mapping-canadian-governments-telecommunications-surveillance/; Michael Geist, "How Telcos and ISPs Hand Over Subscriber Data Thousands of Times Each Year Without a Warrant", April 1, 2014, MichaelGeist.ca, http://www.michaelgeist.ca/content/view/7100/135/; Order/Address of the House of

Commons, “Responses to Written Question Q-233 - Ms. Borg (Terrebonne-Blainville)”, march 24, 2014, et seq, http://www.christopher-parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.

[18] Bill S-220, An Act to Establish the Intelligence and Security Committee of Parliament, October 16, 2013, 62 Elizabeth II, 41st Parliament, 2nd Session, 1st Reading, http://www.parl.gc.ca/content/hoc/Bills/412/Private/S-220/S-220_1/S-220_1.PDF. Bill C-551, An Act to Establish the National Security Committee of Parliamentarians, November 7, 2013, 62 Elizabeth II, 41st Parliament, 2nd Session, 1st Reading, http://www.parl.gc.ca/content/hoc/Bills/412/Private/C-551/C-551_1/C-551_1.PDF.

[19] Michael Geist, “Why CSEC and CSIS Should Be the Subject of an Independent Investigation”, January 8, 2014, MichaelGeist.ca, http://www.michaelgeist.ca/content/view/7043/135/.

[20] Re X, 2013 FC 1275, https://www.canlii.org/en/ca/fct/doc/2013/2013fc1275/2013fc1275.html. See also: Re X, 2009 FC 1058, https://www.canlii.org/en/ca/fct/doc/2009/2009fc1058/2009fc1058.html and Re CSIS Act, 2008 FC 301, https://www.canlii.org/en/ca/fct/doc/2007/2007canlii62002/2007canlii62002.html.

[21] British Columbia Civil Liberties Association, “Spying in Canada: Civil Liberties Watchdog Sues Surveillance Agency Over Illegal Spying on Canadians”, October 22, 2013, BCCLA.org, http://bccla.org/wp-content/uploads/2013/10/Final-Press-Release-Spying-10_21_131.pdf; British Columbia Civil Liberties Association v. Attorney General of Canada, British Columbia Supreme Court File No.: VLC-S-S-137827, October 22, 2013, Notice of Civil Claim, http://bccla.org/wp-content/uploads/2013/10/2013-10-22-Notice-of-Civil-Claim.pdf.

[22] British Columbia Civil Liberties Association, “Illegal Spying: BCCLA Files Class Action Lawsuit Against Canada’s Electronic Spy Agency”, April 1, 2014, BCCLA.org, http://bccla.org/news/2014/04/illegal-spying-bccla-files-class-action-lawsuit-against-canadas-electronic-spy-agency/; Lyster v. Attorney General of Canada, Federal Court File No. T-796-14, Statement of Claim, April 1, 2014, http://bccla.org/wp-content/uploads/2014/04/20140401-Statement-of-Claim-Class-Action-Proceeding.pdf; Omar Ha-Redeye, “BCCLA Files Class Action for Spying by CSEC”, April 13, 2014, Slaw.ca, http://www.slaw.ca/2014/04/13/bccla-files-class-action-for-spying-by-csec/.

[23] Canadian Civil Liberties Association (CCLA), “The Canadian Civil Liberties Association Challenges Constitutionality of Privacy Legislation”, May 22, 2014, CCLA.org, http://ccla.org/2014/05/22/press-release-ccla-challenges-constitutionality-of-privacy-legislation/; Corporation of the Canadian Civil Liberties Association et. al. v. Attorney General of Canada, Ontario Superior Court File No.: CV-14-504139, Notice of Application, May 13, 2014, http://ccla.org/wordpress/wp-content/uploads/2014/05/Notice-of-Application-re-PIPEDA-Issued.pdf.

[24] Bernier, Chantal, “Statement from the Interim Privacy Commissioner of Canada Regarding Telecommunications Companies’ Responses to Information Requests from Government Authorities”, April 30, 2014, Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/media/nr-c/2014/s-d_140430_e.asp, Canadian Wireless Telecommunication Association, “Response to Request for General Information From Canadian Wireless Telecommunications Association (the “CWTA”) Members”, December 14, 2011, http://www.priv.gc.ca/media/nr-c/2014/let_140430_e.pdf; Michael Geist, “Canadian Telcos Asked to Disclose Subscriber Data Every 27 Seconds”, April 30, 2014, MichaelGeist.ca, http://www.michaelgeist.ca/content/view/7116/125/.

Correspondents: Micheal Vonn, Christopher Parsons and Tamir Israel.

Colombia

Snowden's leaks confirmed that many governments in the world are under permanent surveillance. Moreover, according to those leaks, during the last 5 years Colombia was the third-highest priority country in the region for surveillance activities (1). In Colombia, a simple diplomatic note by the Ministry of Foreign Affairs was sent to Washington stating some discomfort over the activities (2).

Shortly after this scandal, the US Secretary of State, John Kerry, visited Colombia and during his press conference it became clear that the incident was considered to be over.(3) Colombia accepted Kerry's explanation that the NSA had acted under established cooperation agreements in keeping with the mutual fight against local guerrilla groups and drug cartels.(4) To no great surprise for Colombian citizens, the meeting between Colombia's President Juan Manuel Santos and Kerry marginalised the issue and the Colombian government further agreed that the activities were done in line with our Constitution and legal framework.(5)

Clearly, during this last year, there has been no official reaction to Snowden's revelations, nor has any public authority demanded any sort of guarantee for citizens from such State surveillance activities, despite the fact that there are real threats by way of recent examples in Colombia. (6)

There is a previous episode that should be considred: the 2009 "DAS wiretapping" spy scandal.(7) The former State Intelligence Agency (DAS in Spanish) illegally tapped the communications of journalists, politicians, judges and NGOs. The facts remain obscure but the incident culminated in the entity's disappearance (many of its officials passed to the new Security Agency and others are now working as freelancers (8). But, after Snowden, the spy scandals returned in 2013, when the media drew attention to "PUMA", the communications-monitoring platform for criminal investigations and key for the implementation of the Intelligence Act.(9) At the time, it became evident how little was known about the new Colombian intelligence institutional framework and State mass and selective surveillance. However, in February 2014 President Santos announced a revision of the Intelligence legal framework (10) triggered by a new revelation exposing a military intelligence

facade operation called “Andromeda.”(11) Once again, the target of State surveillance activities were mainly journalists, political opponents, government and guerrilla peace negotiators in La Habana. The language describing the initial impact of the proposed revision soon changed from reviewing the intelligence legal framework to enhancing the State cyberdefense.

If Snowden's revelations have had some influence in Colombia it was to highlight the fact that intelligence decisions cannot be based solely on State security rationale. To some extent, these revelations have served to demonstrate that there are limits to state surveillance activities. It has also shown that there is a need to guarantee citizens' rights, as well as to establish civil society oversight mechanisms. Yet, it will take some time to translate this recognition to the domestic reality.

References:

1. Colombia, el tercer país más espiado en la región
http://www.eltiempo.com/archivo/documento/CMS-12920262

2. EE.UU. debe explicar espionaje en Colombia: Cancillería
http://www.semana.com/nacion/articulo/eeuu-debe-explicar-espionaje-colombia-cancilleria/350271-3

3. John Kerry defends NSA surveillance programs in Latin America
http://www.huffingtonpost.com/2013/08/12/john-kerry-nsa_n_3745886.html

4. Presidente Santos pide explicaciones a Estados Unidos en caso de espionaje
http://www.elcolombiano.com/BancoConocimiento/P/presidente_santos_pide_explicaciones_a_estados_unidos_en_caso_de_espionaje/presidente_santos_pide_explicaciones_a_estados_unidos_en_caso_de_espionaje.asp

5. Jhon Kerry defendió los programas de NSA
http://laopinion.com.co/demo/index.php?option=com_content&task=view&id=426284&Itemid=29

6. Risks of an uncontrolled state surveillance in Colombia
http://karisma.org.co/?p=3900

7. Colombian intelligence service wiretapped journalists
http://www.cpj.org/2009/02/colombian-intelligence-service-wiretapped-journali.php

8. El DAS a la sombra y otros tenientes visibles
http://www.caracol.com.co/noticias/actualidad/el-das-a-la-sombra-y-otros-tenientes-visibles/20140204/nota/2070530.aspx

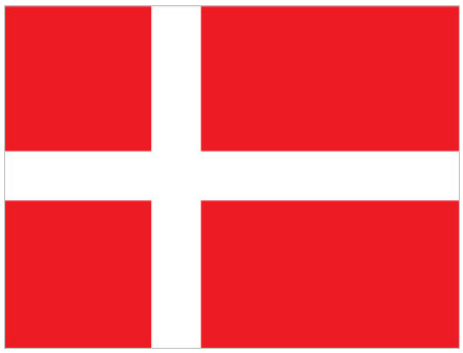
9. PUMA: amenazas a la intimidad y a la libertad de expresión

http://razonpublica.com/index.php/politica-y-gobierno-temas-27/6929-puma-amenazas-a-la-intimidad-y-a-la-libertad-de-expresion.ht

10. With New Unchecked Surveillance Revelations, Colombian Government Ignores Both History and Human Rights https://www.eff.org/deeplinks/2014/04/new-unchecked-surveillance-revelations-colombian-government-ignores-both-history

11. A new wiretapping scandal casts doubt on the Colombian military\u8217\'19s support for peace talks http://www.colectivodeabogados.org/A-new-wiretapping-scandal-casts

Correspondents: Carolina Botero, Pilar Saenz and Amalia Toledo from Karisma Foundation



Denmark

Since the first Snowden revelations became available in June 2013 there has some activity in Denmark with governmental, political and judicial responses to questions asked by media and NGOs. But the overall observation is that none of these debates actually led to any changes in attitude for the vast majority of parties in the Danish Parliament - the *Folketinget*.

Only one small leftist party, Enhedslisten, took a critical stand, while the rest of the parties supported an often repeated statement from the Government: *"We have no reason to believe, that any illegal American intelligence activities directed toward Denmark or Danish interests are taking place."*[1]

Media Coverage of the Snowden revelations has in general varied over time. Niche media in Denmark did cover some of the initial stories. [11,12]

By January, 2014, media coverage seemed to peak, especially when details about the the top meeting COP 15 in Copenhagen were released in January.[13] The remainder of 2014 has seen a decline in coverage.

No judicial or legislative initiatives have been carried out to prevent mass surveillance or limit access to company and personal data as a consequence of the Snowden revelations. On the contrary, there have been initiatives to further legalise and legitimise the current modus operandi - as carried out by intelligence services operating in Denmark or on behalf of Denmark.[2, 3]

1. The Centre for Cyber Security operated by the Danish Defence Intelligence Service [4]

The Center has been operational for two years. New legislation is to be introduced by June, 2014, allowing mass retention of log data and communications data without prior court warrant. The new law is expected to be finally approved by Danish Parliament by mid June. [5,6] According to the legislative proposal, Intelligence authorities may decrypt intercepted communications and distribute the content to foreign intelligence services. [7]

2. Danish Administrative Order for data retention

In December 2013 the Court of Justice of the European Union concluded that the Data Retention Directive is incompatible with the Charter of Fundamental Rights. The Danish Department of Justice and Minister of Justice, Karen Hækkerup, opined that the EU Court decision had no consequence with regard to the Danish Administrative Order. [10]

However on June 2nd. the the Danish Minister of Justice, Karen Hækkerup declared, that the extensive logging of traffic was to stop within a couple of weeks. "It is doubtful if the collection of session data can be regarded as suited for achieving the purpose of creating possibilities for use of the information as part of an investigation of criminal activities", a press release from the Danish Department of Justice stated.[18]

By phrasing the reasons for shutting down the log files, The Minister avoided coupling the decision to any of the criticism received and left a door open to introducing more effective procedures for collecting session data in the future. Furthermore: How the already collected data will be handled is still uncertain.

3. Self censuring in ITEK

ITEK is a part of the Confederation of Danish Industry (DI). [14] The body represents some 300 companies working with IT, Telecom, Electronics and Communications, and issues an annual report about recent security threats and advice to protect companies and individuals against industrial espionage.

This year the first edition of the report was dropped due to internal criticism. The second edition was published and only available for two days before it was dropped and now a third edition is in the works, though it's unknown which fate it will meet when published. It has been suggested, that censoring has taken place and terms such as "GHCQ", NSA" and four pages of text on Snowden have been significantly edited out of the various editions. Newspaper Politiken has revealed that changes took place after a confirmed meeting between ITEK and the Danish Defence Intelligence Service. [15, 16, 17]

NOTES

[1] Meeting 47 Danish Parliament 2013-14
http://www.ft.dk/samling/20131/forespoergsel/f8/beh1/forhandling.htm?startItem=56
[2] FE, Danish Defence Intelligence Service http://fe-ddis.dk/eng/Pages/English.aspx

[3] Danish Security and Intelligence Service, Politiets efterrentingstjeneste
[4] http://fe-ddis.dk/cfcs/omos/opgaver/Pages/Opgaver.aspx
[5] Minister: Fin balance i ny lov om cybersikkerhed
http://politiken.dk/indland/ECE2227381/minister-fin-balance-i-ny-lov-om-cybersikkerhed/
[6]Hemmelig tjeneste får magten over private data
http://politiken.dk/forbrugogliv/digitalt/ECE2225888/hemmelig-tjeneste-faar-magten-over-private-data/
[7]Law Proposal of May 2nd, 2014 by Minister of Defence, Nicolai Wammen - Forslag til Lov om Center for Cybersikkerhed
http://www.ft.dk/samling/20131/lovforslag/l192/html_som_fremsat.htm
[8] http://en.wikipedia.org/wiki/Data_Retention_Directive#Criticism
[9]Ekspert efter EU-dom: Logning bør suspenderes
http://www.information.dk/493873
[10] http://www.b.dk/politiko/haekkerup-vil-ikke-aendre-overvaagningsregler-trods-eu-dom

[11] https://www.prosa.dk/aktuelt/prosabladet/artikel/artikel/giv-snowden-nobels-fredspris/?tx_prosamag_pi1[pageid]=5438
[12] http://www.information.dk/463313
[13] http://www.information.dk/486285

[14] http://di.dk/English/Pages/English.aspx

[15] Fire sider om Snowden blev slettet i vejledning fra Dansk Industri
http://politiken.dk/indland/ECE2251274/fire-sider-om-snowden-blev-slettet-i-vejledning-fra-dansk-industri/
[16] DI drøftede omstridt vejledning med spiontjeneste
http://politiken.dk/indland/ECE2280839/di-droeftede-omstridt-vejledning-med-spiontjeneste/
[17] Second, withdrawn version of report from ITEK
http://multimedia.pol.dk/archive/00834/Scan_834583a.pdf (Newspaper Politieken).

Correspondent: Kurt Westh Nielsen

Finland

Despite widespread media coverage of the Snowden disclosures, there have been few concrete actions by politicians to end surveillance, and practically no concrete outcomes.

Media coverage of the disclosures has been extensive, and the reaction has been mostly pro-whistleblowing. Reporting has been largely US/NSA focused; spying by other countries or the local national Government didn't receive so much press (but see below for the related national cybersecurity programme). There has been some investigative journalism: the main Finnish newspaper Helsingin Sanomat published a lengthy investigative report on "Nokia Lumia phones leaking information to foreign countries [that is, the US]" (2014). Helsingin Sanomat also published an objective analysis of the Snowden material it obtained; due to Snowden's cautious publication policy, the most sensitive material was not available.

Greenwald's book (2014) on the disclosures is available in Finnish.

There has been no significant public action such as demonstrations or large campaigns that have triggered a measurable impact. The citizens' legislative initiative "Lex Snowden" ("law for protecting privacy and free speech internationally", including whistleblower protection) supported by Effi received 4 179 supporters out of 50 000 required for the initiative to be processed by the Parliament.

Some members of the Parliament have, for example, mentioned the Snowden disclosures in their speeches. However, there have been no formal investigations, resolutions or other such actions with tangible outcomes, although there have been public debates that may have affected legislative processes.

There have been no disclosures-related cases brought before courts, police or judicial authorities.

There are no concrete indications of positive future reforms in the Finnish cybersecurity arena. Since 2013, police authorities have expressed their wish

to obtain surveillance rights similar to those provided by Sweden's FRA legislation. (1)

The Government (except certain ministers/ministries) has taken no action to improve legislation as a result of the Snowden disclosures.

The execution programme (11 March 2014) of the Finnish national cybersecurity strategy shows an inclination to undermine online privacy and extend state surveillance to confidential communications. A few months after the first Snowden disclosures, cyber attacks on the Ministry of Foreign Affairs were publicized (2013). Consequently, work for a new online surveillance legislation draft commenced: security officials requested more power to monitor online communications. The group that wrote the draft consisted solely of officials; the majority of them were national security authorities. The Ministry of Transport and Communication organized a public debate, where several participants criticized the draft. (2)

In another public debate (April 2014) on the proposed cyber surveillance legislation, industry representatives were mostly anti-surveillance, while security officials were pro-surveillance. (3)

A proposed legislative package on the information society (30 Jan 2014) contained no reaction to the disclosures. Instead, there were plans to incorporate old requirements on telecom data retention in the package, also extending the requirements towards communication content retention and a centralized storage model.

The Government has not publicly announced how the Digital Rights Ireland ruling by the EU court will affect said legislation. Fortunately, some politicians have reacted positively to the ruling. For example, the Minister for Education and Science promised that the ruling's effects on Finnish legislation shall be examined in order to repeal those parts of legislation that are in conflict with the ruling. (4)

Some companies have used Finland's alleged privacy-friendliness as a marketing point for ICT services such as cloud-based services; this is at least indirectly related to the Snowden disclosures.

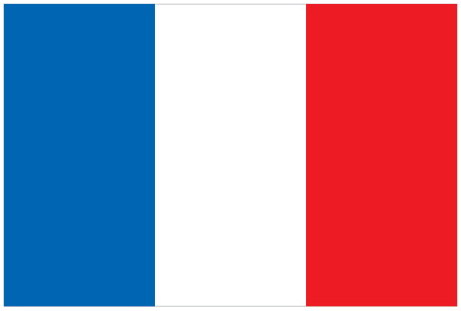
(1) http://www.talouselama.fi/uutiset/supo+haluaa+seurata+sinua+tarkemmin+verkossa/a2191293

(2) http://www.itviikko.fi/uutiset/2014/01/21/kybertiedustelulaki-kuumentaa--yritykset-ja-jarjestot-eivat-mukana-valmistelussa/2014993/7

(3) http://www.taloussanomat.fi/uutiskommentit/2014/05/03/uusi-paha-urkintalaki-vai-pienen-suomen-suojakilpi/20146096/12

(4) http://www.lvm.fi/tiedote/4395687/eu-tuomioistuin-totesi-tietojen-sailyttamista-koskevan-direktiivin-laittomaksi

Correspondents: Ville Oksanen, Lauri Hirvonen, Niklas Vainio, Otso Kassinen, Electronic Frontier Finland.



France

The Snowden revelations have caused in France the same schizophrenic uproar that occurred after the NSA/Echelon scandal fifteen years ago. At first, the reports caused a general outcry in media and political circles, but soon after the revelations about French surveillance capabilities were put into light, the outcry silenced and all legal suits that were launched against the US-led SIGINT spying apparatus came to nothing.

In 2013, French Foreign Minister Laurent Fabius made his first public statement more than three weeks after the first Snowden revelations (PRISM). He urged an “official explanation” from the US, as echoed by other major European leaders, after newspapers Der Spiegel and The Guardian reported how the NSA had targeted its spying inside EU institutions.

The only major diplomatic gesture taken by Laurent Fabius took place on October 21, 2013, when he stated he had “called immediately” the US Ambassador for a special meeting. That gesture came after daily newspaper Le Monde published new documents from the Snowden files showing how massive was the scale of NSA spying of French special interests.

Just after the first Guardian article on June 5, media columnists and major political figures urged the French government to ask for official explanations. Some argued for the opening of Parliamentary inquiries. In fact, these special investigation powers — like the one that was launched in Germany, for instance — were never engaged in the French Parliament (National Assembly and Senate). Not even a single MP dared to merely propose a resolution that would have created a “commission d'enquête”. Some left-wing MPs recently quoted the NSA-led spying scheme, explaining that it must be stopped as a “prelude” to pursuing talks regarding the Transatlantic treaty. In fact, French Socialist EuroMPs — allies to the French President Hollande — declared on July 1st that the inquiry should be led by the European Parliament. The “*Committee of Inquiry on Electronic Mass Surveillance of EU Citizens*” was launched four days later.

The only move by the French Parliament occurred recently, on May 22, 2014. The Law Commission of the Senate organized public hearings of public

security and civil rights experts for a conference called “Numérique, renseignement et vie privée : de nouveaux défis pour le droit” (Digital issues, intelligence and privacy: new challenges for the legal system).

Regarding the PRISM scandal, the French judiciary opened a preliminary inquiry on August 28, 2013, responding to a lawsuit launched by the civil rights group FIDH (International Federation of Human Rights Groups). The preliminary suit is still pending (the second step would be the opening of an official judicial inquiry).

Last November, newspaper Le Monde published details of how the French intelligence services deployed similar sniffing techniques in order to store and analyse huge quantities of phone and internet metadata for internal use.

The French Data Protection Agency (CNIL), which is currently head of the “Article-29” EU privacy working party, failed to put minds at rest when it published shy memos regarding PRISM’s legal impact on internet users in France. All of CNIL's initiatives now, are engaged in the A-29 inquiry, launched on August 20, 2013.

Ironically, the only legal consequences of the Snowden/NSA files was not good news for France's citizens and foreign residents. A “military programmatic law” — prepared in July 2013 and voted in December — introduced new metadata surveillance measures, including geo-tracking capabilities, for the intelligence community. Security experts said all these measures were often used in law. Another “geo-tracking” law was adopted at the end of March 2014, aimed this time at judicial bodies, in order to similarly “legalise” localisation techniques already used by police in day-to-day investigations. The “Snowden earthquake”, as this scandal has been called here, seems to have helped French authorities to clean its Criminal Code, more than it contributed to build a better privacy shield for ordinary people.

Correspondent: Jerome Thorel.

The European Union

The Snowden revelations generated a great deal of noise in the discussions around privacy, security and data protection. However, in the absence of any specific decision-making process (apart from the Data Protection Regulation), much of the reaction was in the form of platitudes.

On July 2013 Justice Commissioner Viviane Reding announced a review of the Safe Harbor Agreement, which was adopted in order to permit transfers of personal data in a way which was recognised by the EU as being compliant with the 1995 Data Protection Directive. This review led to the creation of thirteen recommendations that Commission Vice-President Reding sent to her US counterparts to address some of the flaws of the agreement.

As the failings of Safe Harbor were already an open secret, it is difficult to determine how much influence the revelations created. However, judicial redress for EU citizens, both as part of an update of Safe Harbor and in the context of a planned umbrella agreement on data protection in the law enforcement sector, are currently being negotiated between the EU and the US. While this latter agreement has been collecting dust in the Commission's drawers since the negotiations started back in 2010, the Snowden revelations have heavily contributed to a relaunch of the talks, as evidenced by the strength of a letter from Commissioner Reding to the US Attorney General in reaction to the PRISM revelations.

However, a more comprehensive - albeit non-binding - response came from the European Parliament. From September 2013 to February 2014, the European Parliament's inquiry received testimonies from tech experts, whistleblowers, journalists, privacy experts, representatives of EU members states and EU intelligences agencies and a written testimony from Edward Snowden. Subsequently, the Parliament has adopted a report which includes seven recommendations intended to guarantee more robust protections of EU citizens' fundamental rights.

The revelations also had an impact on the draft Data Protection Regulation being negotiated in the European Parliament. In particular, in the aftermath of the disclosures on the PRISM programme, Members of the Parliament proposed modifying the Data Protection Regulation in order to reinsert Article 42, the so-called “anti-FISA clause”. Safeguards had been included in an early draft of the Commission's proposal for data protection rules, which said that authorities in third countries could have access to EU data only if the transfer was covered by a specific legal agreement. These safeguards were deleted from the final version of the proposal published in January 2012 because of lobbying by US authorities. This article has been successfully reintroduced and adopted by the European Parliament last March under the new Article 43.a.

The European Court of Justice had to rule on a case on the legality of the data retention regime in the ten months following the Snowden revelations. It is impossible to assess if, or how much, this context may have influenced the Court. However, the outcome was a ruling which overturned an invasive surveillance measure and which cast several more such instruments and planned instruments into doubt.

The Snowden disclosures hit a nerve for many EU politicians, undermining trust in their Transatlantic cohorts. However, apart from the additional and limited safeguards in the Data Protection Regulation, the revelations have largely been limited to rhetoric on the challenges of preserving fundamental rights in the digital age. It remains to be seen whether these words can be translated into meaningful reform.

Correspondents: Joe McNamee and Raegan MacDonald

Germany

The Snowden leaks entered the public sphere in the middle of the German electoral campaign and filled the news extensively for most of the summer and until late autumn 2013. The media impact was quite extraordinary considering the usual niche character of news with a digital dimension and put all acting politicians under pressure. However according to opinion polls conducted before the elections, the leaks were a minor concern for most citizens. [1]

All private and public television channels, the biggest newspapers in both their print and online versions (Spiegel, FAZ, Sueddeutsche Zeitung, Zeit, ZDF, ARD, RTL, etc.) [2] reported vastly from summer until November 2014. Since January 2014 on, the German media regularly publishes editorial articles or news on political reactions to the Snowden leaks with a main focus on the US governmental actions and operational technicalities of the NSA programs.

The Spiegel is one of the few media outlets in possession of original leaked material worldwide. They are still examining undisclosed material along with the help of Jacob Appelbaum and Laura Poitras and their news is mainly focused on the technical aspects of diverse programs implemented by the NSA. On a smaller scale, media reported on the involvement of the German Intelligence Agency (BND). However, since May 2014 the focus on the nature and degree of cooperation between the BND and the NSA is becoming more present due to the commencement of duties of the committee of inquiry on the NSA at the German Federal Parliament (Bundestag) [3].

In autumn of 2013 the *Freiheit statt Angst* (freedom not fear) demonstration gathered between 10.000 and 15.000 people on the streets of Berlin. It was organised by multiple civil society organizations, but its impact was largely limited to circles attached to Internet issues. This demonstration was not the first of its kind, but was larger than the years before. [4]

The demonstrations and the calls for petition signing did not have a significant impact. The most successful campaign was the petition to Chancellor Angela Merkel over change.org demanding a more adequate political response to the NSA-Leaks. It reached 75.000 signatures [5]

The Bundestag established a committee of inquiry into the NSA on the 20th of March 2014. It started its work in April 2014 and has had one hearing session with specialist evidence in May 2014 [6] so far. The committee has been appointed for the 18th legislative session and is scheduled to run for approximately three years.

The federal prosecutor started an examination of the case on the 27th of June 2013 [7]. On the 4th of June the federal prosecutor announced the initiation of a preliminary investigation against persons unknown with regards to the tapping of Angela Merkel's mobile phone. Allegations on massive surveillance against the German population are still under examination [8].

Additionally a politician of the Pirate Party in Bavaria (Marcus Dinglreiter) presented a criminal complaint that was dismissed by the Regional Prosecutors of Bamberg and Coburg for judicial reasons. Since the prosecutors had tried to close the case without sufficient investigation of the facts, Mr. Dinglreiter was able to turn the matter into a forced complaint procedure. The Regional Prosecutor of Bamberg (Bavaria) is now responsible for investigating the case on the basis of strong suspicion [9].

Also, the Chaos Computer Club filed on the 3rd of February 2013, a criminal complaint with the Federal Prosecutor General's office. No outcomes or official statements have appeared since then [10].

The German chancellor appointed after the elections, an additional state secretary to account exclusively for the secret services. The Ministry of Interior and the Ministry of Economic affairs and Energy also presented a joint progress report in August 2013 with a list of measures for better protection of the private sphere. [11]

Part of the measures consist of international talks with the US or the European partners concentrated on issues such as the European data protection regulation and the UN International Covenant on Civil and Political Rights. However, national intelligence agencies are specifically excluded both in European data protection regulations and also in the Covenant.

According to the report, the German BND is in talks with other EU intelligence agencies and is drafting cooperation standards. No further information on this issue has been published since August 2013.

The administrative agreements made 1968/1969 on the G-10 Laws regulating German intelligence agencies and the cooperation between the US, France and the UK with respect to the privacy of correspondence, posts and telecommunications have been annulled. But according to the former Minister of the Chancellery, the cooperation between the NSA and the BND was made on the basis of a secret Memorandum of Agreement from 28. April 2002. [12]

In addition, a new IT Security Law had been foreseen before the Snowden revelations, but it had been strongly resisted on economic grounds due to

provisions on a proposed obligation to report security incidents. The progress report announced a new drafting proposal as one of the measures for better privacy protection against global threats. The draft is finished and under governmental consultation [13]. This legal initiative originated a new narrative within the German private sector, driving new business model concepts based - among other ideas - on national or regional routing.

A new addendum to the government procurement laws was announced in May. According to several interviews, [14] the law amendment is designed to ease the burden of proof in favour of the German government towards non-German companies. One key outcome is that the transmission of industrial and business secrets to third parties may lead to a contract annulment in case of discovery through reliability testing. While this would certainly be a measure that aims to provide for more transparency, it does not necessarily equate that all contracts with non-German companies will be cancelled if transmission to third parties is disclosed. The annulment would depend on consideration by the German government.

Civil society organisations like *Reporters Without Borders Germany, Human Rights Watch, Whistleblower Netzwerk, Digitale Gesellschaft* and others have repeatedly asked the German government and parliament to step up its investigation into the case, esp. citing a lack of transparency. This was the case for the issue of asylum for Snowden with an interlinked possible hearing by the parliamentary inquiry committee as well as questions on the extent to which civil society organisations have been monitored and what the government plans to do about this. Until now, there have been no official answers by the government. [15]

To our knowledge, most industry associations have been quiet; organisations like eco (Internet-Industry) have no public statements or position papers on their website, while big companies like Deutsche Telekom and 1&1 Internet AG attempt to profit from the NSA Scandal through programs like *national routing* and "*E-Mail Made in Germany*". *"The NSA-Scandal comes in handy, we should embrace it as a chance [for the German economy"* said Markus Kerber, from Germanys biggest industry association (BDI). [15b]

Some smaller E-Mail providers like *posteo.de* issued transparency reports on government data requests (the first of such kind in Germany) which then triggered Deutsche Telekom to follow suit. No coordinated effort to reform which data can be shared as a result of intelligence requests has been seen so far. [16]

———

[1] cf. the graphics of Infrastest made during the German electoral campaign (in German) bit.ly/1twVFC8

[2] http://www.spiegel.de/thema/nsa_ueberwachung/

[3] For more information visit the homepage of the committee (in German) www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss

[4] Here some press reports: http://www.google.com/url?q=http%3A%2F%2Fwww.spiegel.de%2Fnetzwelt%2Fnetzpolitik%2Ffreiheit-statt-angst-2013-demonstration-gegen-nsa-ueberwachung-a-920927.html&sa=D&sntz=1&usg=AFQjCNEaEA99fzZ7XfISOOJlxmrGqsJ59w

[5] The change.org petition can be found here (in German): www.change.org/de/Petitionen/bundeskanzlerin-angela-merkel-angemessene-reaktion-auf-die-nsa-aff%C3%A4re

[6] The reports of the three experts on the first hearing session can be read here (in German): www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848

[7] Press report (in German): www.sueddeutsche.de/politik/spaehaffaeren-bundesanwaltschaft-soll-verfahren-wegen-spionage-pruefen-1.1738018

[8] cf. (in German) www.mz-web.de/politik/bundesanwaltschaft-prueft-ermittlungen-zur-nsa-affaere,20642162,23903482.html and www.aljazeera.com/news/europe/2014/06/germany-probe-merkel-phone-bugging-201464123350342688.html

[9] see the press release at of Mr. Dinglreiter (in German) piratenpartei-bayern.de/2013/09/27/pirat-sorgt-fuer-ermittlungsverfahren-im-nsa-skandal/

[10] Press release of the CCC ccc.de/de/updates/2014/complaint and http://www.racf.de/PM%20Strafanzeige%20NSA.3.2.14.pdf

[11] Read the progress report (in German) here: www.bmwi.de/BMWi/Redaktion/PDF/S-T/massnahmen-fuer-einen-besseren-schutz-der-privatsphaere,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

[12] Read the press statement of former Minister of the Chancellery Pofalla (in German): www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/08/2013-08-12-pofalla.html

[13] For the draft visit (in German) www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html#a-info-1 and for more on the official position of the German Government on the draft of the new IT-Security Law see e.g. the speech of the vice-president of the BSI (German Agency for Security and Information Technique), Andreas Koennen, (in German): www.tele-task.de/archive/lecture/overview/7774/

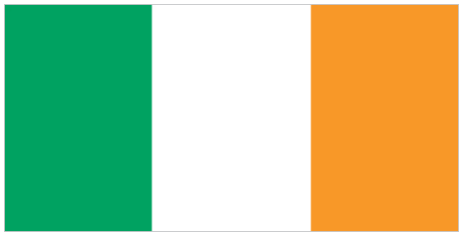
[14] cf. www.egovernment-computing.de/commerce/articles/446309/

[15] https://www.reporter-ohne-grenzen.de/nc/pressemitteilungen/meldung/keine-aufklaerung-ohne-transparenz/ and https://www.reporter-ohne-grenzen.de/nc/pressemitteilungen/meldung/offener-brief-an-die-bundeskanzlerin-zur-sicherheit-edward-snowdens-in-deutschland/ and https://www.reporter-ohne-grenzen.de/themen/kampagnen/whistles-for-whistleblowers/

[15b] http://www.faz.net/aktuell/feuilleton/it-sicherheitsgipfel-die-nsa-affaere-kam-wie-gerufen-12765364.html

[16] c.f. Transparency reports:
https://posteo.de/site/transparenzbericht_2013 and
http://www.telekom.com/sicherheitsbehoerden

Correspondents: Lorena Jaume-Palasi and Hauke Gierow



Ireland

The Edward Snowden revelations have had little impact in Ireland, despite the fact that Dublin is home to European headquarters of many of the Internet firms targeted by the NSA and GCHQ [1]. While there has been extensive media coverage, there has been no concrete action by the Irish government or parliament to investigate the abuses and the Data Protection Commissioner has refused to examine disclosure of information by Facebook under the PRISM programme [2]. To the contrary, the government has signaled its willingness to assist the US government in the extradition of Mr. Snowden [3]. The response of the Irish government has been marked by an unwillingness to antagonise the United States, rather than any desire to protect the privacy of Irish citizens.

Media reporting

For the most part, Irish media coverage has been confined to reporting and commenting on material revealed elsewhere. There does not appear to have been any investigative journalism considering, for example, the possible involvement of Irish authorities, the role of subsidiaries of US firms or the extent to which Irish undersea cables might have been tapped. With some honourable exceptions [4], there has been little media interest even examining the response of the Irish government.

Public action

There have been no large-scale demonstrations or online campaigns against US surveillance.

Cases before courts and other authorities

On 4 July 2013 the Irish Attorney General, acting on a request made by the US government, sought a pre-emptive extradition arrest warrant against Mr. Snowden before the High Court [5]. When that warrant was refused by the court (on the basis that the location of the alleged offences had not been established), the Minister for Justice went on to say that:

> *“The Irish and US authorities have remained in close contact about this matter and, for its part, the Government will take any action open to it to ensure that the State's obligations in relation to extradition arrangements are met.” [3]*

Following the Snowden revelations, Max Schrems of Europe v. Facebook made a complaint to the Data Protection Commissioner regarding Facebook's involvement in the PRISM programme. Mr. Schrems sought a formal investigation of access by US authorities to personal data transferred from Facebook-Ireland to Facebook Inc. in the US. [6] The Data Protection Commissioner refused to carry out an investigation on the basis that the European Commission's "Safe Harbour" decision prevented him from examining the actions of US authorities in relation to data transferred under Safe Harbour. Mr. Schrems brought a judicial review against that refusal, and a decision is now pending from the High Court. [7] Whatever the outcome of that decision, the case highlights an important gap in European practice, which currently does not seem to have an effective mechanism to examine abuse of European citizens' data when transferred abroad.

Government and parliamentary action

The Irish government has made only token protest to the US and has not investigated possible breaches of Irish law. As summarised by the political correspondent of the Irish Times:

> *"It is beyond dispute that the Coalition is collectively reluctant to shout or complain too loudly or make any probative inquiries as to whether the bugging and covert surveillance that has occurred in Germany, France and elsewhere has happened in Ireland." [4]*

Individual opposition and backbench members of parliament have raised the issue, but the Irish parliament has not held any formal inquiry, debate or vote prompted by the Snowden revelations.

Professional organisations

There does not appear to have been any formal response by any of the professional bodies (such as those representing lawyers and doctors) which one might expect to safeguard the privacy of communications.

Reforms

There is nothing currently on the table prompted by the Snowden revelations; however a number of domestic factors including possible police abuse of surveillance powers and the success of Digital Rights Ireland in challenging the Data Retention Directive may collectively lead to some reform of national law in the mid term. [8] [9] [10]

[1] Jamie Smyth, "Dublin becomes hub for major internet groups", Financial Times, 27 October 2011, http://www.ft.com/intl/cms/s/0/836bffd0-00a8-11e1-930b-00144feabdc0.html.

[2] Derek Scally, “Ireland: prisoner of Big Tech?”, Irish Times, 3 May 2014, http://www.irishtimes.com/news/technology/ireland-prisoner-of-big-tech-1.1781833.

[3] “Statement by Minister for Justice, Equality and Defence, Alan Shatter TD, on judgement in the case of an application for a provisional arrest warrant in relation to Edward Snowden”, 8 July 2013, http://www.justice.ie/en/JELR/Pages/PR13000279.

[4] Harry McGee, “Government parties show divergent views on spying issue”, Irish Times, 1 November 2013, http://www.irishtimes.com/news/politics/government-parties-show-divergent-views-on-spying-issue-1.1579693.

[5] Attorney General v. Snowden [2013] IEHC 308, http://www.bailii.org/ie/cases/IEHC/2013/H308.html.

[6] Noel Baker, “Judicial review of Facebook PRISM case to be heard this week”, Irish Examiner, 28 April 2014, http://www.irishexaminer.com/ireland/judicial-review-of-facebook-prism-case-to-be-heard-this-week-266720.html.

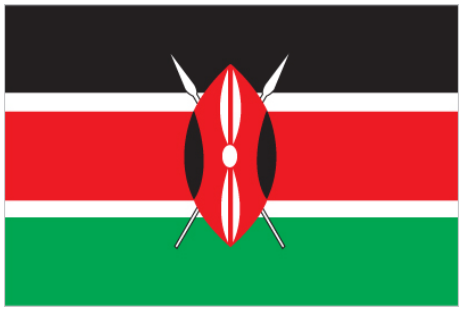
[7] Mary Carolan and Genevieve Carbery, “Data Commissioner decision challenged by Facebook user”, Irish Times, 29 April 2014, http://www.irishtimes.com/news/crime-and-law/courts/data-commissioner-decision-challenged-by-facebook-user-1.1777930.

[8] C-293/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General http://curia.europa.eu/juris/documents.jsf?num=C-293/12

[9] Conor Lally, “Bugging found at offices of Garda complaints watchdog”, Irish Times, 9 February 2014, http://www.irishtimes.com/news/crime-and-law/bugging-found-at-offices-of-garda-complaints-watchdog-1.1685345.

[10] Stephen Collins, Conor Lally and Fiach Kelly, “Government fears recording of phone calls at Garda stations may threaten convictions”, Irish Times, 26 March 2014, http://www.irishtimes.com/news/politics/government-fears-recording-of-phone-calls-at-garda-stations-may-threaten-convictions-1.1738206.

Correspondent: TJ McIntyre



Kenya

The overall impact of the revelations by Snowden[22] on NSA's surveillance in Kenya[23] is that there has been very little discussion from Kenyans. This can be noted by the few Kenyan media reports[24] on the same or online discussions on the impact of the revelations on Kenyans. This is despite Kenyans having a right to privacy under the 2010 Constitution of Kenya under Article 31, that states:

> "*Every person has the right to privacy, which includes the right not to have— (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed*."

We can also note that the 2010 Constitution of Kenya requires that the Parliament legislates on a Data Protection Bill but we can note that it is yet to be legislated upon. We can also note that Kenyan internet is ranked as free[25], but there has been evidence of Blue Coat Devices capable of filtering, censorship, and surveillance.[26]

Scale and nature of media reporting

The nature of media reporting in Kenya was mostly a reproduction of news[27] from major international news agencies with viewership/ readership in Kenya such as CNN, Aljazeera, the Guardian, and New York Times among other international media. Most of the reports did not address local/ national

---

[22] https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

[23] https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

[24] http://www.standardmedia.co.ke/mobile/?articleID=2000121935&story_title=Kenya:%20wikileaks-us-eavesdrops-on-kenyans-calls

[25] http://www.freedomhouse.org/report/freedom-net/2013/kenya

[26] http://www.academia.edu/3534690/Planet_Blue_Coat_Mapping_Global_Censorship_and_Surveillance_Tools

[27] http://www.businessdailyafrica.com/Corporate-News/Kenya-key-target-as-NSA-infiltrates-Huawei-/-/539550/2257126/-/1mc9fa/-/index.html

involvement in surveillance and was primarily focused on the US and the NSA as a single entity except one.[28]

Actions taken

We can note that in Kenya there has not been any consequent public action in the manner of demonstrations or large-scale campaigns that had a measurable impact.[29] There have not been any reported cases brought before courts, police or judicial authorities regarding privacy or data protection.

We can however note that the Kenya Human Rights Commission and other civil society organizations have organized public awareness forums on protecting oneself online and there have also been discussions about privacy on mailing lists but these have not been very conclusive.

Reform for the future?

In January 2014, Telecommunications industry regulator, Communications Commission of Kenya (CCK), announced new regulations that gave it unfettered access[30] to private or confidential information on consumers without a court order.

The powers, which are contained in a new set of regulations that has been prepared for publication in the *Kenya Gazette*, allow the CCK or its agents the leeway to obtain information or data held by telecoms operators.

We can note that even the above incident did not capture media attention in Kenya apart from a single media outlet and a few blogs.

This is also not the first time that the regulator is mentioned[31] in an attempt at infringement on privacy[32] - all in the name of cyber security.[33]

In Kenya there is no hard evidence that there will be a future development that will bring reform or transparency to the security arena given the major telco in Kenya is openly building a surveillance system for the government and this has not met a major call for transparency from the company.

Correspondent: Ephraim Percy Kenyanito

---

[28] http://www.thejackalnews.com/politics/kenyan-security-agencies-also-unlawfully-intercept-your-phone-calls-and-emails

[29] http://www.nation.co.ke/oped/Letters/The-spying-ogre-will-eat-all-of-us-including-MPs-/-/440806/2159394/-/a8a7rg/-/index.html

[30] http://www.businessdailyafrica.com/CCK-trashes-telecom-users--privacy-with-new-spying-rules/-/539546/2152122/-/15ltdyoz/-/index.html

[31] http://allafrica.com/stories/201205181170.html

[32] http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/item/2/-/edcfmqz/-/index.html

[33] http://www.trending.co.ke/cck_pushes_firms_to_host_websi-336840453.html

Mexico

In June 2013 – one year ago - Edward Snowden revealed to the world the true extent of the United States National Security Agency's generalised espionage throughout the world. When news started to break out in Mexico, there was at first no reaction from the government - even though some of Snowden's documents detailed in the press showed that espionage involved the country directly. In September 2013, the Brazilian newspaper *O Globo* wrote, based on confidential documents disclosed by Edward Snowden, that the NSA had illegally wiretapped the communications of then Mexican presidential candidate, Enrique Peña Nieto, as well as some members of his cabinet (1). In October 2013, the German weekly *Der Spiegel* published a report, also based on Snowden's documents, which explained that the NSA had intercepted e-mails from Mexico's ex-President, Felipe Calderón, and the Office of the President, as part of the operation "*Flatliquid*". The newspaper had also obtained access to emails of various officials at the Ministry of the Interior (Secretaría de Seguridad Pública), which is in charge of fighting against drug trade and human trafficking, in an operation called "*Whitetamale*" (2).

As part of the *O Globo's* revelations, in one of the documents Snowden revealed to journalists, Mexico appears on a list of countries entitled "*Friends, Enemies or Troubles?"* while, in another, the importance of spying Mexico regarding trade issues is specifically mentioned. *O Globo* also stated that slides Snowden released indicate the U.S. had been making efforts gathering information on energy policy in Mexico (3) while *Der Spiegel* pointed that the NSA had not only obtained information about drug cartels, but also economic and political information.

Reactions in Congress

Many Congressmen condemned the NSA's espionage, considering it an intrusion into Mexico's sovereignty. In July 2013, the Congress adopted a resolution (4) that opposed the espionage by the NSA and any action that violates Mexican citizens' right to privacy and data protection or infringes the sovereignty of Mexican diplomatic delegations. Although the resolution criticised the potential violation of all Mexican citizens' privacy, Congress limited itself to demand that the Federal Government ask for explanations to the US Government about the spying activities of Mexican public officers and diplomatic delegations and requested the US to stop these activities immediately and permanently. The PRD political party had asked that Congress include a request – eventually not included in the resolution – to issue a report about spying practices and ask information from the US government about the collaboration agreements signed between the Mexican and US governments. (5)

The Government's reaction

In July 2013, the Ministry of Foreign Relations (*Secretario de Relaciones Exteriores*) condemned the violation of the confidentiality of the communications of Mexican institutions, declaring that espionage violates international laws. That same Ministry sent a letter of protest to its counterpart in the United States, requesting a thorough investigation that clarify responsibilities and implement corrective actions. President Obama thereafter committed to his Mexican counterpart to start an exhaustive investigation. (6)

On 15 January 2014, the Ministry of Public Administration (*Secretaria de la Función Pública*) signed a framework contract with companies, including Google and Microsoft, in order to acquire from them software licenses until 2016, despite the fact that those companies were precisely the ones found to have collaborated with the NSA and to have been the target of espionage by the same agency. This represents a reaction different than what occurred in other countries such as Sweden, where authorities have prohibited the use of Gmail and other Google applications on government platforms, and Brasil, where the government decided to develop its own tools to avoid using private communication systems based in the United States or offered by US companies. (7)

On 8 May 2014, the Ministry of the Interior (*Secretaría de Gobernación*) and the Ministry of Public Administration issued new rules applicable to all public servants regarding the storage and management of data centers based in public institutions' own premises, and the processing of sensitive 'national security' data, under an "information security government model". (8)

Academics and companies' reactions

Various academics (9), criticised the Government's attitude, saying that they had been too timid, and, instead, praised the Brazilian Government's reactions (10) (11). Mexican state-owned petroleum company, Petroleos Mexicanos (PEMEX) (12), which together with the Brazilian petroleum company Petrobras (13), have both been spied by the NSA, did not issue any statement; neither did private companies based in Mexico. While US companies, such as Apple, Yahoo, Google, Twitter, Microsoft, Netflix and Cisco, did oppose the NSA espionage in the U.S., their Mexican subsidiaries did not make any comments. National organisations, trades unions, professional associations and industry groups didn't release any press release either.

In the media

Despite the gravity of Snowden's revelations, most national media did not cover them extensively. However, efforts by civil society had some impact as thousands of Internet users protested against surveillance and espionage through social networks.

Civil Society's reactions

NGOs such as *ContingenteMX* and *SonTusDatos* joined and supported various campaigns aimed at opposing NSA's espionage and its impact for human rights in Mexico. As an example, those two organisations, together with dozens of other NGOs around the world, sent a letter to the US Congress (14) and another one to US President Barack Obama (15) to oppose the NSA's illegal surveillance practices.

On 21 June 2013, 3 Mexican activist organisations, *ContingenteMX*, *Propuesta Civica* and

Al Consumidor, filed a complaint before the Federal Institute of Access to Information and Data Protection (IFAI) in order for the governmental authority to investigate Mexican servers that have allegedly hosted a spyware named "FinFisher" that might violate the country's privacy and data protection legal framework and individuals' human rights (16). The investigation is still in progress.

On 11 February 2014, NGOs, including *ContingenteMx* and *SonTusDatos*, and companies such as Mozilla México and *Wikimedia México*, as well as Internet websites such as Nodo9 and *Sopitas*, joined the international campaign "The Day We Fight Back" to oppose NSA's espionage (17). Beside these, no other actions and campaigns have been carried out in Mexico.

The public's reaction

During legislative discussions earlier this year about the reform to the telecommunications legal framework, thousands of people in the street, and many more online, urged Congress to protect their rights to privacy, data protection and freedom of expression from the Federal Government while congress members were debating the bill the government had submitted.

Social network users and NGOs, among others, have rejected that telecommunications bill because, among other things, the text, as it is currently drafted, mandates telecommunications providers to help the government obtain users's geo-location data in real time without any judicial due process and to retain all of their communications' meta-data for two years. (18) The bill is still in discussion in Congress.

Conclusion

What Snowden revealed about the US government's espionage generated diverse reactions in Mexico. On the one hand, the Mexican government has shown a rather passive attitude towards the NSA's invasion to its citizens' privacy. On the other, the way Mexican civil society organisations have reacted has been decisive in nurturing more awareness among Mexicans about their entitlement to claim more respect from the government to their right to privacy. This awareness has been displayed in how the public reacted to the government's telecommunications reform bill.

(1) The NSA had had unauthorized access to many emails, mobile phone calls and text messages of him and his closest collaborators. See C. Tardáguila, "EUA espionaram Dilma", O Globo, 1 September 2013, http://oglobo.globo.com/pais/eua-espionaram-dilma-9782118.

(2) "Kerry: Spying 'not unusual' in international relations", BBC, 1 July 2013, http://www.bbc.com/news/world-us-canada-23129690.

(3) "Report: NSA spy program focused on Latin America Oil, Energy Programs", CBS DC, 9 July 2013, http://washington.cbslocal.com/2013/07/09/report-nsa-spy-program-focused-on-latin-america-oil-energy-programs/.

(4) Segunda Comisión de Trabajo de la Comisión Permanente del H. Congreso de la Unión, Relaciones Exteriores, Defensa Nacional y Educación Pública, Dictamen con Punto

de Acuerdo relativo al programa de espionaje de la Agencia de Seguridad Nacional estadounidense, 31 July 2013, http://sitl.diputados.gob.mx/LXII_leg/dictameneslxii_pa.php?tipot=%20&pert=&idacut=576; http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=42275.

(5) A Congressmember also proposed to increase from 5 to 15 years of prison the penalty for those who carry out espionage through telecommunications by interfering with, stopping or intercepting wire, wireless or optic fiber communications. He also proposed to sanction those who sell equipment, devices or other computing equipment that enable the interception of communications by any electronic means over public telecommunications networks. The proposal, however, did not go through. See Chamber of Deputies, Histórico de Comunicación Social, 1 November 2013, http://www3.diputados.gob.mx/camara/005_comunicacion/b_agencia_de_noticias/009_2013/11_noviembre/01_01/4852_plantea_sanchez_torres_reformar_el_codigo_penal_y_castigar_con_hasta_15_anos_de_prision_a_quien_realice_espionaje_a_traves_de_redes_de_telecomunicacion.

(6) "Obama se compromete con Peña Nieto a investigar espionaje," Excélsior, 5 September 2013, http://www.excelsior.com.mx/nacional/2013/09/05/917194.

(7) Julio Sánchez Onofre, "Google, Microsoft y Oracle, primeros ganadores de la Estrategia Digital," El Economista, 6 March 2014, http://eleconomista.com.mx/tecnociencia/2014/03/06/google-microsoft-oracle-primeros-ganadores-estrategia-digital.

(8) "Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias," 8 May 2014, DOF, http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014. See also Korina Velázquez, "Nuevo MAAGTICSI: Emiten políticas para la Estrategia Digital Nacional en TIC y seguridad de la información", Agenda Digital, 12 May 2014, http://agenda-digital.info/2014/05/12/nuevo-maagticsi-emiten-politicas-para-la-estrategia-digital-nacional-en-tic-y-seguridad-de-la-informacion/.

(9) Academics such as Eduardo Rosales Herrera, PhD. in International Relations and René Jiménez Ornelas, PhD. in Social Sciences, both professors at the National Autonomous University of Mexico (UNAM).

(10) E. Olivares, "'Tibia, sumisa y temerosa' reacción de México a espionaje de EU: especialistas", La Jornada, 9 September 2013, http://www.jornada.unam.mx/2013/09/09/politica/017n1pol. In turn, at 2 conferences promoting a new reference deskbook about cloud computing, published in September 2013 and that had been fully financed by Microsoft, its author, Julio Tellez, another professor from the UNAM, did not mention anything about Snowden's revelations about the NSA's espionage and how they could have impacted the development of cloud-related services in Mexico – neither did other government and industry and trade associations' representatives present at those events. The person responsible for the Mexican Presidency's National Digital Agenda, Alejandra Lagunes, speaking on behalf of Presidency did, however, mention the importance of protecting the country's national security and Mexican citizens' personal data, but without referring to Snowden's revelations.

(11) Daniel Gershenson, Director of the NGO Al Consumidor, produced a video where he contrasted the reactions of Brazil and Mexico. The video makes a summary of the news and points at the different tones of the reactions in Brazil and Mexico. "El espionaje de Estados Unidos en México. Daniel Gershenson", Revolución tres punto cero, 23 October 2013, http://revoluciontrespuntocero.com/el-espionaje-de-estados-unidos-en-mexico-daniel-gershenson/.

(12) D. Brooks, "La NSA ha espiado a Pemex, Petrobras y petroleras de Arabia Saudita e Irán," La Jornada, 22 May 2014, http://www.jornada.unam.mx/2014/05/22/mundo/023n1mun.

(13) J. Watts, "NSA accused of spying on Brazilian oil company Petrobras", The Guardian, 9 September 2013, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

(14) SonTusDatos, "SonTusDatos firma carta al Congreso de Estados Unidos sobre Internet y vigilancia de telecomunicaciones," 18 June 2013, http://sontusdatos.org/sontusdatos_firma_carta_para_congreso_eeuu_sobre_internet_y_vigilancia_telecomunicaciones/.

(15) SonTusDatos, "SonTusDatos hace un llamado al Presidente de Estados Unidos para que proteja a los denunciantes y periodistas", 14 August 2013, http://sontusdatos.org/sontusdatos_hace_llamado_al_presidente_de_eeuu_para_que_proteja_a_denunciantes_y_periodistas/.

(16) El software ha sido presuntamente usado en varios países para espiar a activistas de derechos humanos. Algunos activistas mexicanos incluso han reportado haber sido espiados. La ONG Privacy International, establecida en Reino Unido, envió una carta al IFAI apoyando la petición de ContingenteMX, Propuesta Cívica y Al Consumidor. Ver B. Jiménez, "Denuncian activistas cacería cibernética," Criterio, 11 July 2013, http://www.criteriohidalgo.com/notas.asp?id=180404.

(17) SonTusDatos, "El Día que Contraatacamos (11 Feb. 2014)," 11 February 2014, http://sontusdatos.org/el-dia-que-contraatacamos/.

(18) Andrea Becerril, "ONG: viola derechos la iniciativa de ley secundaria en telecomunicaciones de Peña," La Jornada, 5 April 2014, http://www.jornada.unam.mx/2014/04/05/politica/013n1pol; SonTusDatos, "Iniciativa de ley secundaria de telecomunicaciones: retroceso para los derechos fundamentales en México", 22 April 2014, http://sontusdatos.org/iniciativa_ley_secundaria_telecomunicaciones_retroceso_para_derechos_fundamentales_en_mexico/.

Correspondents: Cédric Laurant, Korina Velázquez and Monserrat Laguna Osorio

Private sector

The corporate sector is inextricably intertwined in the revelations about widespread secret government surveillance programs. The first document published on June 5th 2013 was a court order to telecommunications provider Verizon demanding the company turn over all call records on an "ongoing, daily basis." The next day, a set of slides was published that accused several leading companies including Google, Facebook, and Apple of close relationships with the NSA. Companies were then forced to dive right in to the conversation.

Before Snowden, there were very few known instances of a corporate entity challenging the NSA's legal authority to conduct spying activities. A then-unnamed company (since revealed to be Yahoo!) challenged the Protect America Act in 2007-2008, and it was recently reported that in 2010 Sprint had raised questions regarding the NSA's bulk telephony metadata program.

In the post-Snowden world, companies have been more vocal than ever in opposition to government surveillance. A still-unknown telecommunications company filed a motion early in 2014 asking for the FISA Court to explain the legal rationale behind Section 215 bulk telephone metadata court orders (the court responded in March). Security firm Cisco is one of many companies that have publicly chided the U.S. government over its extensive surveillance activities. French telecom company Orange threatened to sue the NSA for wiretapping undersea fibre optic cables, but has not yet followed through.

In fall 2013, investors filed resolutions asking AT&T and Verizon to release "transparency reports." Pioneered by Google, and now issued by most major internet companies - particularly in the wake of the Snowden revelations - these reports provide statistics and policies on requests for user data, content removal and other actions impacting privacy and free expression. While the telecoms sector has historically been conspicuously silent on issues of state access to user data, both AT&T and Verizon complied and issued transparency reports, and Vodafone, CREDO Mobile, Deutsche Telekom, Telstra, Comcast, and others have followed suit.

In late 2013, several major internet companies teamed up to create the "Reform Government Surveillance" Coalition. This initiative, which coalesced around an open letter to the U.S. President and Congress, supports five guiding principles around surveillance activities, including authority, oversight, and transparency. In May of 2014, Google sent an action alert to users who had previously taken action on digital rights issues, urging them to "demand real surveillance reform," of the U.S. Senate, following the passage of an extremely watered down version of the USA FREEDOM Act -- originally the most promising proposal for NSA reform -- by the U.S. House of Representatives.

Company data security policies have also been impacted by revelations of mass surveillance resulting in improved security for users. Services geared toward providing anonymity and confidentiality while using the Web and internet have become more popular than ever before. For instance, use of Tor, an anonymous browsing network, doubled between October 2012 and October 2013. Digital rights group Access launched the Data Security Action Plan (DSAP) in March 2014, and several companies, including Twitter, Golden Frog, and Silent Circle, joined in "Supporting" the adoption of these seven steps toward a more secure Internet. The DSAP was intended to move the public conversation beyond transparency to talking about tangible steps companies can take to secure the data they hold and prevent unauthorized access to user data. Yahoo!, long a laggard on digital security, announced several new security features in response to revelations, including greater traffic encryption for email and searches. In March 2014, Google publicly announced that all traffic between its data centres would be encrypted and that all email messages would be routed over encrypted channels.

The role of the corporate sector in facilitating government mass surveillance has come into focus after the Snowden disclosures. Many companies have taken steps to increase the security of their networks and transparency around the troves of data they collect. There is, however, still much more progress to be made.

Correspondents: Amie Stepanovich and Peter Micek

Netherlands

The Snowden revelations have seen little to no effect in the Netherlands. Most significantly, the proposal to give the Dutch intelligence services similar powers as the NSA has been delayed for a few months.

As everywhere, the first Snowden revelations made headlines in the Dutch media. However, most of these reports did little more than translate the output of the original story. After a couple of months. as the audience became bored with the same story time after time, the amount of attention declined considerably. The revelations on Dutch involvement were highly anticipated and turned out to be somewhat of an anti-climax. As a result, attention was quickly lost. In the end, the most critical and extensive analyses were made by spare-time bloggers.

The Dutch government's response to the revelations has been extremely weak: ambiguous answers, systematic denial and avoiding any strong position. Whenever possible, the government pointed towards Europe for a response. The reason for this lack of outrage is evident: the Dutch intelligence services have close ties to their American and British counterparts. The debates within the parliament have been fierce, but rarely profound. A report of the intelligence services oversight committee on the use and sharing of information by the intelligence services has been critical about the trust-based cooperation with the NSA, amongst other points.

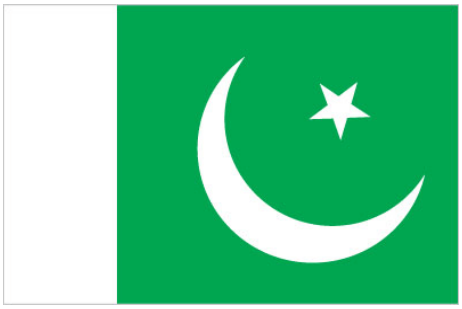
The Snowden revelations coincide with a review of the Dutch law governing the intelligence services. The most striking part of this review is the introduction of a massive and untargeted wiretap competency, similar to the powers of both the NSA and the GCHQ that were highlighted by Snowden. British intelligence is quoted in one of the leaked documents stating "*the Dutch have some legislative issues and they need to work through before their legal environment would allow them to operate in the way that GCHQ does" and that GCHQ is "providing legal advice.*" The proposal for the new powers is, at best, delayed by the Snowden revelations, but it's definitely not

off the table.

The most notable event outside of politics and media is the law suit against the Dutch State, brought forward by a coalition of NGO's and citizens. The coalition demands a prohibition of the use of data of others by Dutch intelligence services if this data has not verifiably been obtained in accordance with Dutch law. Their proceedings made clear the government misinformed the general public and the parliament, almost leading to the resignation of the responsible minister.

Possibly the best result of Snowden's revelations: citizens and companies are slowly realizing they should turn to themselves for protection against government snoops. There is a considerable rise of crypto parties, where research journalists and ordinary citizens are taught how to protect one's online communications.

Correspondent: Rejo Zenger,



Pakistan

The leaks from NSA whistleblower, Edward Snowden, did not initially attract local attention in Pakistan. This situation, however, changed on September 1, 2013, with the publication of a leak specifically pertaining to Pakistan. A Washington Post report had revealed that the U.S. intelligence agencies intensely focus on Pakistan (a U.S. ally), to the same extent that it scrutinises adversaries such as Iran and North Korea. This disclosure triggered uproar and discomfort both in political and in civil society sections of the country.

This situation had a devastating impact on the free speech narrative in Pakistan, which was already marred as freedom of speech and expression are largely seen as a western motion. The extent to which the NSA spied on civilians across the world further polarised the debate for open access in Pakistan. Activists now fight the argument that *"if the citizens of United States of America can't have these rights; how can you?"*

The NSA leaks did not have any major impact on Pakistani policies or legislation until very recently (as discussed below). Local media has focused primarily on U.S. and the NSA at the centre of surveillance issues. Despite the primary focus, media does cover, from time to time, local updates, legislations, and civil society calls for banning surveillance in the local fora especially after the finding of FinFisher's presence in Pakistan.

Pakistan did not see any massive scale public demonstrations against the human rights abuses that Pakistan is involved in (as leaked in the report), or NSA snooping over Pakistani government and agencies. However, this did not deter civil society groups from organising online. Under the flagship of *The Day We Fight Back*, civil society organised a local campaign titled *Jasoosi Band Karo* was strategised to push the government for better policies to protect citizen privacy and stop mass surveillance.

Even though there are no policies in place now, efforts have been made to respond to the NSA leaks, Pakistani Senator Mushahid Hussain in April 2014 presented a bill titled the National Cyber Security Council Bill (NCSC) in the Senate against the revelations of intrusion into privacy and spying by

overseas intelligence networks. The NCSC bill presents a formulation of a national level council with functions and powers to develop and draft policy and governance models with the emerging cyber security threats.

This Draft bill seeks to take institutional steps to combat one of the major non-traditional, non-military threats the country is facing. If the Council draft bill is passed by the parliament, it would result in the establishment of a dedicated mechanism specifically assigned to draft policies, guidelines and strategies on cyber security issues. NCSC will also allow the council and its members to monitor relevant legislations and devise strategic plans with a ten and twenty-year vision in accordance with international best practices.

The Cyber Security Council bill appears on the surface to be a progressive step towards formulating and strengthening policies around cyber security. However, while the bill emphasises the facilitation of communications between government, academia and corporate entities, it has clearly no provision for recognising human rights activists or civil society entities working on digital security. This is essentially what makes the bill rxtremely worrisome.

This draconian bill in its current form authorises Council and its members with enormous powers with little or no opportunity for challenge. The bill also lacks any provisions on safeguarding citizens' privacy and freedom of expression while the council conducts its functions.

There have been no specific court cases related to the NSA revelations. However, the existing cases brought against Pakistan over its use of the FinFisher spy suite and over blocking YouTube for an indefinite duration have not yet seen any tangible outcomes. Yet, these efforts have made headway into creating more awareness regarding these issues, developing case law and highlighting the importance of amicus to support litigation concerning human rights issues. Civil society activists also consider that forcing government to the court actually alienates the government further from working alongside activists.

Pakistan is yet to see any major development in terms of transparency and accountability in the country, however improved net security legislation and privacy bills are expected to be introduced.

Correspondents: Nighat Dad,* Sana Saleem *and Shaikh Rafia

Poland

In Poland, Snowden's disclosures concerning the National Security Agency's mass surveillance programs did not result in any meaningful political reactions. From the very beginning of this scandal it was clear that among most influential decision makers there was no political will to respond to the alleged cooperation of Polish agencies with American counterparts or demand explanations regarding the surveillance of Polish leaders. Neither the government nor Polish society visibly opposed US practices or demanded explanations and the stopping of mass surveillance (1).

Even though Polish media broadly reported Snowden's disclosures, that coverage has not led to a significant public outcry in Poland. Human rights advocates and the tech community were quite isolated in their demands for more information and more accountability. Parliamentary commissions responsible for democratic oversight in the area of national security and foreign policy didn't bother to invite members of the government for a hearing. Even opposition leaders who would normally be the first ones to criticise the government this time remained silent (2). In the midst of public debate triggered by his disclosures, Snowden's request for asylum in Poland was rejected. Minister of Foreign Affairs Radosław Sikorski announced his decision on Twitter, claiming that Edward Snowden did not provide all needed documents to start asylum procedure.

In October 2013 three human rights organisations – Panoptykon Foundation, Helsinki Foundation for Human Rights and Amnesty International Poland – filed 362 FOIA requests containing very detailed questions about Polish involvement in US mass surveillance programmes, international cooperation among intelligence agencies, political reactions to Snowden disclosures and measures adopted by Polish authorities to protect the secrecy of their communication. Until now they have not received answers to the key questions because relevant information was treated as classified or was simply refused on the ground that government bodies do not have such knowledge (3). However, one aspect has been confirmed by Polish authorities in their responses: lack of strong political reaction to Snowden's disclosures. Apart from a simple diplomatic note sent by the Ministry of Foreign Affairs in

June 2013, no further steps have been taken. Legal cases concerning the unanswered questions are still pending.

Summing up, there is no indication that Snowden's disclosures will bring any substantial changes in rules governing cooperation among intelligence agencies or the responsibility of internet service providers for sharing data with such agencies in Poland. On the other hand, undoubtedly these disclosures have had a positive impact on public awareness concerning blanket surveillance of telecommunications and its human rights implications.

1) Bodnar, K. Szymielewicz, *Poland's citizens need to know the impact of Prism on their lives*, The Guardian, 16 October 2013, http://www.theguardian.com/commentisfree/2013/oct/16/poles-prism-poland-surveillance-threat;

2) K. Szymielewicz, Silence remains the easiest answer, openDemocracy.org http://www.opendemocracy.net/can-europe-make-it/katarzyna-szymielewicz/silence-remains-easiest-answer-polish-nonreactions-to-snow

3) Panoptykon Foundation, 100 questions on surveillance to Polish authorities, http://panoptykon.org/node/6598

Correspondent: Katarzyna Szymielewicz

South Africa

South Africa is physically a great distance from where Edward Snowden made his revelations – but these revelations nevertheless struck home. In South Africa, the plight of whistleblowers is of growing importance, with their social, economic and physical safety increasingly under threat.

Snowden's revelations highlighted the escalating powers being bestowed on security agencies shadowed by the broad veil of 'national security concerns'. And South Africa is no different. The past few years have seen a growing centralisation of power by our State Security Agency, and concurrently tightening restrictions on the flow of information - as exemplified in the much-maligned *Protection of State Information Bill.*

Snowden's revelations brought whistleblowing into the public consciousness, and sent a positive image of the impact whistleblowers make. In a country like South Africa, this is invaluable as we struggle to shake off the Apartheid legacy of associating the whistleblower with the 'impimpi' (police informants) – a concept that those with things to hide have abused to keep the knowing silent. Here, corruption is rampant. And the role of the whistleblower has never been more important. But it is only when the common understanding of the whistleblower as a valuable member of an open society becomes broadly accepted, that our work to advance the cause of whistleblowers can gain real traction.

And that traction has begun. In the beginning of April, ODAC and the University of Cape Town's Democratic Governance and Rights Unit co-hosted a multi-stakeholder consultation to shape the course for increased whistleblower protections. South Africa's Public Protector, Advocate Thuli Madonsela (one of Time Magazine's 100 Most Influential People) presented at the meeting – highlighting how the international perception of whistleblowers and the fight against corruption can influence the South African experience.

We have extensively documented the plight of the South African whistleblower. Edward Snowden highlighted the universality of this plight, and has helped to re-invigorate the call to protect all legitimate whistleblowers, as the voices of a vigorous and open democracy.

Correspondent: Gabriella Razzano

Spain

When the Snowden revelations were published in June 5th, 2013 only one Spanish paper, *El Pais,* gave them space on its front cover, but only on June 7th and in the following terms: 'US justifies mass surveillance on security grounds'. What made front cover, then, was the official US reaction and not the revelations.

This caution and privilege of the official response has been the norm in the media debate in Spain. Together with the government dismissal of US surveillance as an issue, this has greatly determined the public debate on the effects of mass surveillance. In mid-June, the Spanish government issued a statement declaring that 'if a citizen is aware that something strange is happening, they should address the national security forces so that an investigation is undertaken'. The Spanish Data Protection Agency, in its turn, declared that EU authorities had already reacted by requesting more information from the US and that this matter had to be dealt with at the continental level.

In July Edward Snowden approached the Spanish government to request asylum, through the embassy in Moscow, and was told that he should be on Spanish soil to process the request (he was in Hong Kong at the time) and that his request had no legal effects due to the procedure used to present it. Shortly after, Evo Morales' presidential plane was denied the right to fly over Spain on the suspicion that he may be travelling with the whistleblower. He was only allowed to refuel in the Canary Islands after Bolivia agreed to the plane being searched - a clear violation of that country's sovereignty.

In spite of this, at the parliamentary level, the Snowden revelations have made their way to Congress, even if always at the request of the opposition and yielding poor results in terms of transparency and accountability. In July 2013 the United Left party filed a series of questions on the possibility for Snowden to acquire asylum status in Spain, and whether any steps had been taken to protect his life and freedom of expression. The government replied in September elaborating on the procedure to request asylum and its compliance with the existing legal framework.

In November 2013 the director of the Spanish Intelligence Centre (CNI) appeared behind closed doors at the Official Secrets Commission. His appearance was agreed after the media revealed that Spain was a 'second degree' ally to the US, and that the CNI had allowed or helped the US tap into 60 million phone calls between December 2012 and January 2013 alone. This was denied by NSA director Keith Alexander, who emphasized that the metadata generated was gathered under regular NATO collaboration and was related only to suspicious activity in third countries (Mali and Afghanistan at least). The members of parliament who attended the Official Secrets Commission were specifically asked not to reveal the details of the session, but those who briefly spoke to the media showed satisfaction and mentioned how the CNI director made it clear that Spain had always acted according to the law, that the data of Spanish citizens has not been compromised or made vulnerable by NSA activities and that it was US intelligence that should provide further explanations.

In December, the left opposition requested permission for Snowden to travel to Spain and appear before the Justice Commission, but the request seems to have been ignored by the government.

In March 2014 the LIBE committee published its report on Electronic Mass Surveillance of EU Citizens, and the left opposition used its recommendations to file a series of questions to the government. Specifically, on April 30th they asked:

> *'What measures have been taken by the government to fulfil the fourteen recommendations of the LIBE committee report on the programs of massive surveillance of the US surveillance agency (NSA)? If the answer is affirmative, what are those measures? If the answer is negative, why?*
>
> *As the report suggests, have the legal measures against the attack on Spain's sovereignty and therefore the violation of general public international law through mass surveillance programs been taken? If the answer is negative, why?'*

The official response form the government may take several months. And while some other parties have expressed their plans to undertake similar actions, as reported recently in *ElDiario.es*, this has not yet happened.

Therefore, while it is difficult to establish a direct link between the parliamentary and the media debate, they both seem to share a lack of interest in the issue. If in Parliament the left opposition is the exception to the rule, in the media mass surveillance has only appeared consistently in the technology section of *ElDiario.es.* The rule, however, continues to be a generalized indifference.

The impact of the Snowden revelations outside of the media and parliament are difficult to assess only twelve months after they happened, even though

this may change in the future. Societal change cannot be measured in such a short time-span, especially when no specific efforts are made in this direction. The Data Protection Agency could have published a report or issued specific materials, but this has not been the case. Also, their 2013 report has not yet been published, and so it is impossible to look for relevant indicators there. The same can be said for the Centre for Sociological Investigations (CIS), responsible for Spain's large opinion polls. The last relevant data we find in their survey series -addressing matters of trust, data protection and feelings of insecurity- is several years old. While this would pose methodological challenges, in the next few years it should be possible to use CIS data to identify trends and changes.

Until then, we can make only educated guesses. The privacy debate in Spain seems to be increasingly conscious of the Snowden revelations and the data protection challenge. In the recent VI Surveillance and Society Conference held in Barcelona and specifically addressing the post-Snowden context, the media were reluctant to cover the event on the grounds of state surveillance alone and seemed to be more willing to link it to data privacy in social media and the responsibility of users. Similarly, the recently opened Big Bang Data exhibition in Barcelona and Madrid relies heavily on the user experience and social media, making few references to Snowden, even though the curators have expressed how the revelations changed their conception of the whole project.

Overall, the Snowden debate seems to be contributing to a more general debate on online privacy and the commercialization of data, while people's expressed concerns continue to focus on unemployment, the crisis and corruption. This is hardly surprising in a post-authoritarian country where top-down surveillance has been the norm rather than the exception for most of the last century, where there is no history of political whistleblowing, where most people confess to being distrustful of their neighbours and where the financial crisis has made all other issues fade into the background. But Spain is also a county that has seen remarkable instances of resistance to CCTV proliferation and where the outcry over whatsapp's data vulnerability did lead to many people looking –somewhat unsuccessfully - for instant messaging alternatives.

There are signs that a debate has been sparked, at least in specific milieus and in relation to cybersecurity, social media and privacy concerns. And while the media and political passivity is an immediate challenge, general privacy concerns have managed to become the standard in technology reporting and policy. In this evolving context, every new revelation on the use and abuse of surveillance powers is contributing to strengthening the need for a true public debate on the possibilities and risks of the surveillance society.

Correspondent: Gemma Galdon Clavell

United Kingdom

Despite facing significant pressure in the wake of the Snowden revelations - one of the largest leaks of classified material in history that revealed the secret mass surveillance apparatus run by GCHQ - the Government has responded with silence, obfuscation and secrecy.

GCHQ is tapping undersea cables, installing spyware onto millions of phones and computers around the world and hacking into the infrastructure of internet service providers. Yet because of the secretive nature of its activities, combined with the weak oversight of intelligence agencies, much-needed policy reforms have been neglected. There is clear evidence that the public opposes such pervasive surveillance, evidenced just over a year ago with the demise of the deeply unpopular Snoopers Charter.

Deputy Prime Minister Nick Clegg has ordered an “Obama-style” review of intelligence agencies, to be led by the Royal United Services Institute, but the report will not even be released until after the May 2015 elections. When it is made public, advocates believe the review should recommend the six principles laid out by the Don’t Spy On Us coalition in the UK:

1 No surveillance without suspicion
2 No more secrecy: Surveillance laws must be transparent and governed by a clear legal framework.
3 Surveillance must be sanctioned by an independent judge, not ministers
4 Effective government oversight
5 A right to redress and have legal challenge heard in an open court
6 overnment ensuring that the web is secure and promote, not undermine, strong encryption.

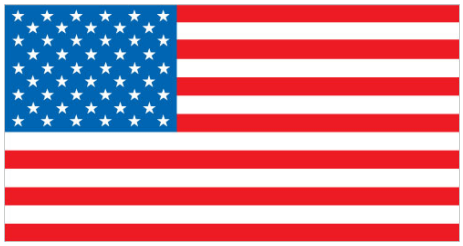
The surprise and outrage shown by politicians at the start of the Snowden leaks died quickly. Nowadays, the only officials we hear from are those charged with oversight of MI5, MI6, and GCHQ, but their words are only ever in defence of the vast and intrusive surveillance conducted by UK authorities. The oversight and review bodies, Committees and Commissioners alike, have produced nothing more than a “Job well done” bouquet to intelligence and security agencies.

This lack of oversight, however, has not gone unnoticed, and in fact is one of the most glaring problems the public is calling to be addressed. The Parliamentary Home Affairs Committee released a scathing report and was highly critical of the so-called oversight bodies. It pointed out in strong language that the current oversight of security and intelligence agencies is weak, inadequate and not fit for purpose.

Given that the prospects of politicians initiating policy change are slim at the moment, the most promising chances of reform have come through legal action. Privacy International, Amnesty International, Bytes for All (Pakistan), Liberty, ACLU (with others), and Abdel Hakim Belhadj have all filed complaints in the Investigatory Powers Tribunal. The IPT, however, is not the ideal venue for challenging state power, since it is mainly a secretive court that almost always sides with Government and does not have to publicly justify its opinions. But, this is the only legal avenue granted to reform the surveillance apparatus. Further, Big Brother Watch, Open Rights Group, English PEN, and internet campaigner Constanze Kurz have filed a similar challenge at the European Court of Human Rights.

There is more action to come, though, as Privacy International continues to challenge GCHQ's surveillance operations, specifically their more intrusive methods of hacking into personal phones and computers.

Correspondent: Mike Rispoli



United States

The Snowden disclosures were met with a broad-based outpouring of outrage in the United States, with the criticism focused mostly on the privacy rights of US citizens. Media coverage was generally highly critical, with national media outlets such as the Washington Post, New York Times, ProPublica and Mother Jones publishing some of the disclosed documents. The disclosures also triggered numerous protests and grassroots campaigns, at least 6 lawsuits aimed at stopping NSA mass surveillance and several legislative proposals aimed at modifying NSA surveillance. The disclosures of the NSA's domestic spying programs, particularly the telephone call detail records collection program, have started a national conversation on both domestic and foreign surveillance policies. However, thus far, none of the surveillance reforms have been aimed at stopping the bulk collection of communications of non-US persons.

Legislative Response

Many members of the US Congress expressed outrage upon the disclosure of the call detail records collection program, even though the US has said the legislators were made aware of the program. Several legislative proposals were offered to reform the call detail records collection, some of which sought to end mass data collection, and others which sought to make the existing program legal. On May 22, 2014, the US House of Representatives passed the USA Freedom Act, which would offer mild reforms of the surveillance. The Act will not become law unless approved by the US Senate and signed by the President. None of the proposed laws would reform NSA surveillance of non-US persons outside the United States.

Executive Branch Response

President Obama convened a panel of constitutional law and national security experts to assess the legality and wisdom of the disclosed NSA surveillance programs. In December 2013, that panel issued a 300-page report that concluded that the NSA's programs raised serious constitutional concerns and proposed 46 reforms. Separately, a newly created standing body called the President's Civil Liberties Oversight Board (PCLOB) issued its own report making more focused findings, but in a similar vein.

The President responded by issuing Presidential Policy Directive 28 (PPD 28). PPD 28 generally instructs the US intelligence community to examine its bulk collection programs and recommend to the President whether those programs can be limited in any way. PPD 28 is notable for acknowledging that privacy rights must be respected "regardless of the nationality of the individual to whom the information pertains or where that person resides." PPD 28 then purports to apply the same protections for the dissemination and retention of bulk-collected data that US persons enjoy to non-US persons. However, these protections are neither explicit nor substantial. Moreover, the US has continued to interpret the International Covenant on Civil and Political Rights (ICCPR), of which it is a signatory, as imposing no human rights obligations with respect to extraterritorial surveillance.

President Obama also announced that he would propose legislation to reform NSA surveillance and its oversight by the Foreign Intelligence Surveillance Court. But although the features of such reform have been released, the President has yet to propose specific legislation.

Public Action

Hundreds of thousands of Americans participated in grass-roots efforts protesting the NSA's surveillance activities through events such as the StopWatching.US coalition and The Day We Fight Back, the latter of which was aimed at protecting the privacy rights of both Americans and foreigners. Data has indicated a marked increase in encrypted Internet traffic in the year since the initial Snowden disclosures (See Sandvine Global Internet Phenomena Report, 1H 2014 https://www.sandvine.com/trends/global-internet-phenomena/).

Legal Actions

At least six legal actions were filed as a direct result of the disclosure of the NSA's mass collection of telephone call detail records. So far, one judge has found the telephone call detail records collection program to be unconstitutional, while one has found it to be constitutional. Both of those decisions are on appeal. The other matters await an initial judicial determination.

None of the lawsuits directly challenge the legality of the surveillance programs with respect to surveillance of non-US persons.

Correspondents: David Greene and Katitza Rodriguez

Information about the contributors

Carolina Botero (Colombia). Carolina is a researcher, lawyer, lecturer, writer and consultant on issues related to law and technology. She is leading the Law, Internet and Society group inside the *Karisma* Foundation and is Regional Project Manager for Latin America for Creative Commons. Every week she writes an opinion column at *El Espectador.*
https://twitter.com/carobotero

Bruna Castanheira: (Brazil). Lawyer active in the areas of Digital Law and Intellectual Property, collaborator of the *Oficina Antivigilância* project, research assistant on the Global Internet Program.

Gemma Galdon Clavell, (Spain). Dr. Clavell is a policy analyst working on surveillance, the social, legal and ethical impact of technology, smart cities, privacy, security policy, resilience and policing. She is a founding partner at Eticas Research & Consulting and a researcher at the *Universitat de Barcelona's* Sociology Department. gemma@eticasconsulting.com Twitter @gemmagaldon

Nighat Dad (Pakistan). Nighat Dad is a lawyer having special focus on Cyber crimes, Privacy, surveillance, Internet Law and Policy, technology and human rights and is a founder and director of Digital Rights Foundation, Pakistan Twitter: @nighatdad

Hauke Gierow (Germany). Hauke is head of the Internet Freedom Desk at *Reporters Without Borders Germany* where he focuses his work on digital source protection, surveillance and companies' responsibility for human rights. He holds a Magister Artium in Political Science and Chinese Studies from Trier University and has been involved in a number of civil society initiatives on 'Internet freedom'.

David Greene, (US). David is Senior Staff Attorney for the Electronic Frontier Foundation (EFF).

Lauri Hirvonen, (Finland). Electronic Frontier Finland - Effi defends citizens' digital rights, including freedom of information without censorship, fair terms of use for digital information and freedom to develop and publish open software. Effi aims to raise awareness on free speech, privacy, copyright and online innovation and to influence related legislation. http://www.effi.org/

Tamir Israel (Canada). Staff Lawyer, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic; Advisory Board Member, Privacy International

Lorena Jaume-Palasì (Germany). Lorena is input coordinator on Global Internet Governance issues at Berlin's Internet & Society Collaboratory. Her

main research focus are privacy and anonymity from a legal-philosophical point of view. She is lecturer and a PhD candidate at the department for Political Philosophy of the Ludwig Maximilians University researching about moral conflicts. She occasionally writes at irights.info

Ephraim Percy Kenyanito (Kenya). Ephraim works with AccessNow.org in Kenya

Otso Kassinen, (Finland) Electronic Frontier Finland.

Melih Kirlidog (Turkey). Melih holds a BSc in Civil Enginering from Middle East Technical University, Turkey, an MBA in MIS, and a PhD from University of Wollongong, Australia. After working as an ICT analyst and consultant for over twenty years he is currently working as an academic in Marmara University, Turkey. He is also a member of Alternative Informatics Association, an advocacy group in ICT issues.

Monserrat Laguna Osorio (Mexico). Monserrat is an intern with *SonTusDatos*, and an International Relations and Political Science student at the *Instituto Autónomo de México* in Mexico City.

Cedric Laurant (Mexico). Cedric is the founder of the nonprofit project "*SonTusDatos*", the first and only in Mexico that is dedicated to defend, and advocate for, the right to privacy and data protection (http://sontusdatos.org). He is a data privacy lawyer and public policy expert who has worked for the past 15 years with more than ten nonprofit organisations in Latin America, the United States and Europe.

Raegan MacDonald, (Belgium). Raegan is European Policy Manager at Access (AccessNow.org), Brussels, Belgium

TJ McIntyre (Ireland). Dr. TJ McIntyre is chairman of Digital Rights Ireland and a lecturer in the Sutherland School of Law, University College Dublin.

Joe McNamee, (Belgium) Executive Director, European Digital Rights – EDRi, Brussels.

Peter Micek (US) Peter is Policy Counsel at Access Now. He leads its advocacy with telecoms companies, developing norms to increase respect for telecommunications users' rights worldwide. A lawyer by training, Peter completed a JD at the University of San Francisco School of Law, and in 2010 published "A Genealogy of Home Visits," critiquing suspicionless surveillance of at-risk communities, in the U.S.F. Law Review.

Jenny Ng (Australia). Dr Jenny Ng specialises in Intellectual Property Law, Information Technology Law and eCommerce Law and has been admitted as a lawyer at the Supreme Court of New South Wales. She has taught both Australian Law and English Law in several countries. She has conducted research extensively in the academia and in practice. Jenny is a Board

Member of the Electronic Frontiers Australia and is a Lecturer at Charles Darwin University.

Kurt Westh Nielsen (Denmark). Kurt Westh Nielsen, kwn@prosa.dk, is a journalist that has been covering topics like Privacy, Data retention, Encryption Technologies and Digital Rights since the Mid-Nineties. He has previously held positions as editor and reporter at *Ingeniøren* (Engineering Weekly) the largest technical magazine in Denmark, and Computerworld Denmark. Currently he is Editor-in-Chief at *Prosabladet* (prosa.dk), a magazine targeted at IT professionals in Denmark.

Ville Oksanen, (Finland). Electronic Frontier Finland.

Christopher Parsons (Canada). Christopher received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Postdoctoral Fellow at the Citizen Lab, in the Munk School of Global Affairs with the University of Toronto. He researches state access to telecommunications data.

Shaikh Rafia. (Pakistan). Shaikh is a research associate at Digital Rights Foundation, Pakistan - one of the foremost organisations policing for accessible and free digital spaces and better privacy legislations in Pakistan. She has contributed to various research publications and her work is routinely published in local and international spaces.

John Razen (Brazil), Law researcher (Instituto Beta), masters student in Constitutional Law and Philosophy of Law (Universidade de Brasília)

Gabriella Razzano (South Africa) is a Senior Researcher at the Open Democracy Advice Centre, South Africa.

Paulo Rená: (Brazil) Law researcher (Instituto Beta), activist for online fundamental rights (Movimento MEGA), founder of Partido Pirata, managed the development of Marco Civil da Internet (Ministry of Justice of Brazil).

Mike Rispoli (UK) Mike is communications manager for Privacy International, in London.

Katitza Rodriguez (US). Katitza is International Rights Director for the Electronic Frontier Foundation (EFF).

Gideon Rop (Kenya).

Sana Saleem is an activist and a journalist based in Pakistan. She is director of *Bolo Bhi* and is on the advisory board of The Courage Foundation

Pilar Saenz (Colombia). Pilar is physicist by profession but activist by vocation. She's a free software, open technology and open culture enthusiast. She works in Karisma Foundation as projects coordinator She also participates in *RedPaTodos*, a group that seeks to influence the Colombian legislations to defend an open, secure and collaborative Internet. https://twitter.com/mapisaro

Katarzyna Szymielewicz (Poland). Katarzyna is human rights lawyer and activist; co-founder and president of Panoptykon Foundation – a Polish NGO defending human rights in the context of surveillance society. Vice-president of European Digital Rights. Graduate of the University of Warsaw (Law) and the School of Oriental and African Studies (Development Studies).

Amie Stepanovich. Amie is Senior Policy Counsel at Access and is an expert in domestic surveillance, cybersecurity, and privacy law. At Access, Amie leads projects on digital due process and responds to threats at the intersection of human rights and communications surveillance. Previously, She is serving as co-chair for the forthcoming 2014 Computers, Freedom, and Privacy Conference. Stepanovich has a J.D. from New York Law School, and a B.S. from the Florida State University.

Jerome Thorel (France) Jerome Thorel, video and radio documentarist, investigative reporter for the past twenty years, member of Privacy international's Advisory Board, was also the founder of the French Big Brother Awards for the period 2000-2010."

Amalia Toledo (Colombia). Amalia is a trained historian and lawyer from Puerto Rico. She has served for several years as a researcher on international affairs. In recent times she has worked at international level on human rights issues, most notably on freedom of expression, press freedom and access to information. Currently she works in Karisma as Project Coordinator. https://twitter.com/amalia_toledo

Niklas Vainio (Finland) Electronic Frontier Finland.

Joana Varon (Brazil) researcher and project manager at the Center for Technology and Society - CTS/FGV, where she works on applied research on ICT for development focused on the evolution of an institutional framework for Internet governance capable of enforcing fundamental human rights, particularly the right to privacy and freedom of expression. Understanding the interplay between policy and technological tools to reach these goals, Joana is also a Member of Open Technology Fund Council, of the Advisory Board of the WebWeWant Campaign and editor of the newsletter Oficina Antivigilância.

Korina Velázquez (Mexico) is a co-founder of SonTusDatos, and a public policy specialist in information society issues.

Micheal Vonn (Canada). Policy Director, BC Civil Liberties Association; Advisory Board Member, Privacy International

Rejo Zenger (Netherlands). Rejo is a researcher at *Bits of Freedom*. He focuses on such topics as governmental surveillance, data retention, intelligence service powers and overview and transparency on user data requests by the government. *Bits of Freedom* is a Dutch civil rights organization, fighting from freedom on the Internet.