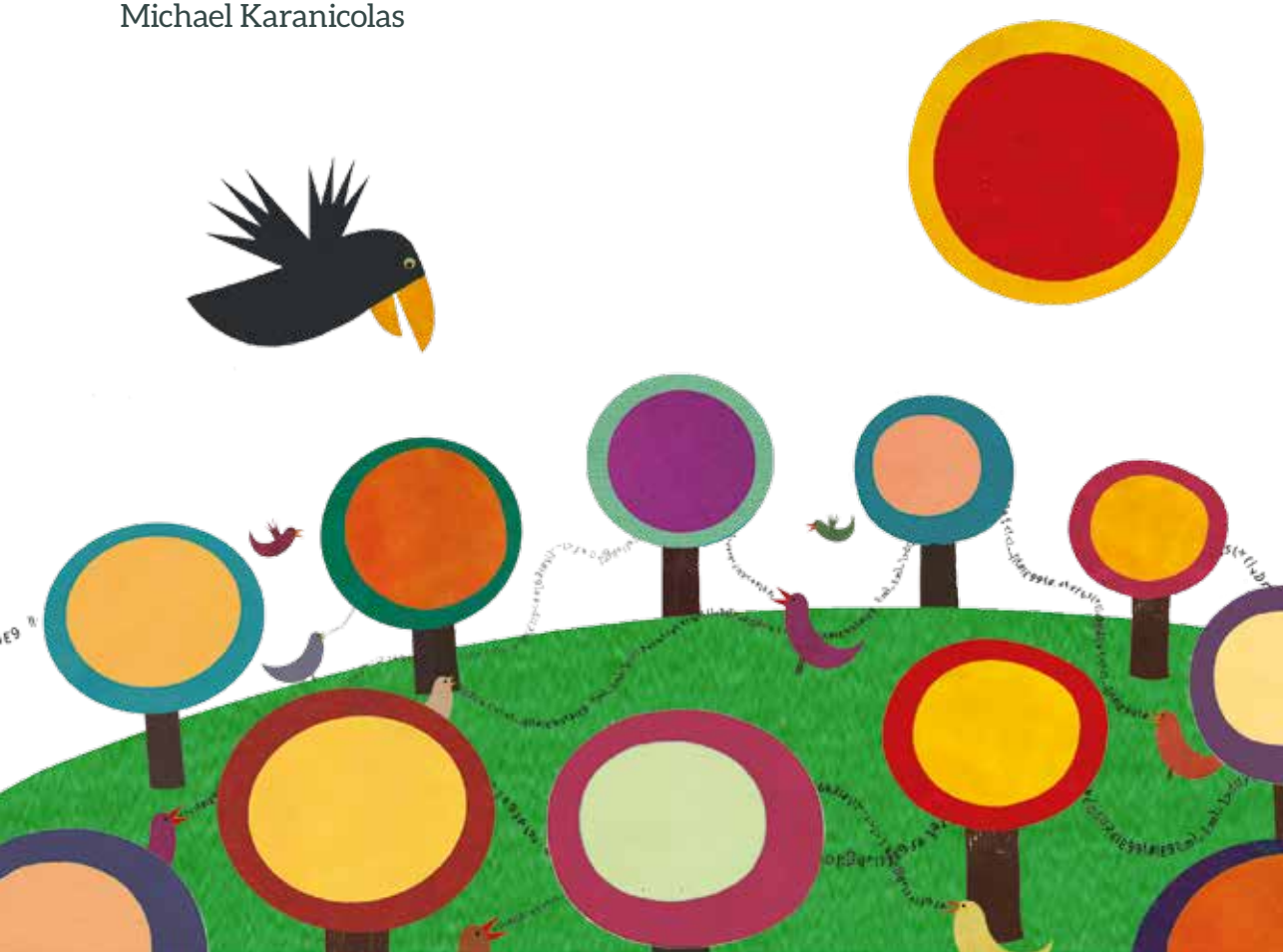
TRAVEL GUIDE TO THE DIGITAL WORLD:

SURVEILLANCE AND INTERNATIONAL STANDARDS

Michael Karanicolas



Published in London 2014
by Global Partners Digital

TRAVEL GUIDE TO THE DIGITAL WORLD:

SURVEILLANCE AND INTERNATIONAL STANDARDS

Michael Karanicolas

"If you look back on the forecasts of surveillance... it turns out that George Orwell was an optimist."

Mikko Hyppönen, Security Researcher
How the NSA betrayed the world's trust - time to act,
October 2013

It is always advisable to do some research before you embark on a trip. A wise traveller will understand their destination before they depart, paying particular attention to any potential security concerns. It may seem strange to apply this advice to the internet, because most people reading this Guide will feel a sense of familiarity, even intimacy, with the online world.

Yet, as the ongoing disclosures by Edward Snowden about surveillance from June 2013 have demonstrated, there is more to the online world than meets the eye. You may be alone in your home or office, but in the online world you most certainly are not. With each new disclosure, fears over the extent of government surveillance continue to mount, while senior officials claim that the leaks are undermining the ability of law enforcement and national security agencies to keep the digital world safe.

In the face of this shifting landscape, it is important to try and understand how surveillance works online, and what privacy and **anonymity** really mean in a digital context.

UNDERSTANDING SURVEILLANCE AND ANONYMITY

For many people, **anonymity** is an important value online as it provides them with a tremendous feeling of freedom. Secret tastes and interests can be pursued and users can express their unfiltered opinions on things great and trivial without fear of what their family or social circle might think. The desire for anonymity can extend beyond protection from social embarrassment to cases where there is a real fear of violence.

The internet's importance in facilitating protest movements against dictatorial regimes in Iran and across the Arab world has been widely documented, but the internet also has an everyday role in freeing its users from restrictive legal or social frameworks. For a gay Ugandan or Russian, or a Saudi atheist, the internet provides the only open avenue for self-expression and for allowing the oppressed to network with likeminded communities.

It is a strange paradox then that, despite its reputation as a safe haven for anonymous engagement, the internet is also the most heavily monitored and tracked medium of expression in history. It is easy to succumb to a comforting perception that one's communications are private. In reality, every move that users make online may be noted, followed and recorded.

In reality, every move that users make online may be noted, followed and recorded.

THE MYTH OF FREE INTERNET SERVICES

Imagine a typical day spent strolling through a shopping centre in your hometown. Perhaps you will browse through titles at a bookstore or record shop, visit your bank or take in a movie. You may see friends or acquaintances and stop to catch up. Now imagine that, for the entire day, there was a group of people following you, diligently writing down every shop you visited and object you looked at and every person you spoke to. Imagine they collated that information to build as detailed a profile as possible about you: your demographic and income level, your hobbies and interests, your political beliefs and so on. Imagine they spent months or years collecting the information, and then offered it for sale to anyone who was interested.

This is essentially the business model that supports an important part of the services offered over the internet. Most companies that offer "free" services online, such as Google and Facebook, derive the bulk of their revenue from advertising and the sale of user information. Rather than paying with money, the people who visit these websites and use these services are, in essence, paying with their private information. As a result, many aspects of the **world wide web** function as enormous data collection mechanisms.

The collection, collation and use of this information, known as **online behavioural tracking**, is a controversial subject. Some types of tracking are considered by many observers to be highly invasive and there is significant debate around the opaque nature of many tracking practices and whether companies are doing enough to seek users' consent before this information is harvested. Obligations to delete user information after a particular time period or upon request and to safeguard information from unauthorised access are also major areas of contention.

On the other hand, it is important to note that this business model underlies many of the free services available over the internet. And tracking does not necessarily negate the value of the internet as a mechanism for anonymous expression. For example, the fact that Google and Facebook know a user's secrets may not inhibit the latter's communications if the information remains hidden from their family, friends and social circle.

CORPORATE SURVEILLANCE VS. STATE SURVEILLANCE

The internet's scope as a mechanism for surveillance has also provided unprecedented opportunities for States to monitor communications, both by requisitioning the data collected by

private companies and through their own, often very extensive, data collection systems. While there are legitimate concerns about the volume of personal information which is collected by private companies, the internet's potential as a data collection mechanism is far more sinister when considered in the context of States. The main reason for this is that the State has a level of coercive power which private companies do not. This is particularly troubling in the case of oppressive governments. For a journalist investigating corruption in Mexico, an Iranian or Chinese dissident or a human rights activist in Russia, marketing agencies are not the threat they need to fear. Even for those who are not obvious targets for State surveillance, the threat of possible criminal measures can exert a **chilling effect** on legitimate speech.

There are other reasons why State surveillance is particularly problematic. Courts and oversight bodies tend to be very deferential to State agencies where questions of national security are raised, giving them far greater leeway than private companies could expect to receive in complying with **data protection** rules. It is also worth noting that private companies face a free market incentive not to be overly intrusive. If a particular website took its **online behavioural tracking** systems too far, it could cost them traffic, something which does not affect security agencies. This is not to suggest that market forces are a substitute for effective regulation, since users' limited ability to engage with and understand privacy policies limits the extent to which invasive policies actually impact a service's user base, but the potential for financial harm can act as at least some sort of check.

ABOUT THIS GUIDE

Having painted a picture of pervasive surveillance, the intention here is not necessarily to demonise the practice or to argue for a total elimination of digital monitoring. It would be absurd to expect law enforcement or national security agencies to do their job without online surveillance. Nobody wants to live in a world where child pornographers, online fraudsters and malicious hackers are allowed to operate freely. What is important is to understand how online surveillance takes place and how it stacks up against international standards relating to privacy and freedom of expression.

This Guide offers a survey of the digital surveillance landscape. Chapter One provides a summary of the surveillance practices carried out by different governments, as far as is known. This includes a particular focus on the **Five Eyes** programmes, where our knowledge has been significantly enhanced by Edward Snowden's revelations. Chapter Two goes on to discuss international standards of freedom of expression and the right to privacy, and their implications in the context of online surveillance. Chapter Three examines ongoing and future debates about surveillance and how the internet is changing as a result of emerging understandings of this subject.

This Guide is aimed at a non-technical audience, so we have also added a Glossary at the end of this guide where words in **bold** print are explained. The Guide does not offer substantive technical advice about how to avoid surveillance, and so we have also included a set of links for Further Reading, which identifies more technical discussions of the issue and websites which host programs or services aimed at evading surveillance.

At the outset, it is important to note that the clandestine world in which intelligence agencies operate makes a comprehensive discussion of this issue impossible. Intelligence agencies around the world operate behind a veil of secrecy, and what we do know is usually the result of leaks or other unauthorised disclosures. Until the Snowden disclosures, virtually nobody outside of the intelligence community had detailed knowledge of the programmes he described. Information about parallel programmes operated in Russia, China and elsewhere remains difficult to come by. But, although a total picture is unavailable, the information we have is sufficient to offer a general understanding of how the system works and why it is problematic.

CONTENTS

CHAPTER 1

WHAT IS DIGITAL SURVEILLANCE?

What Is Digital Surveillance?

ECHELON

The origins of today's sweeping surveillance systems lie in signals intelligence programmes that were founded during the Cold War. The best understood of these was founded in 1971 to target satellite communications. Although the programme has become known to the public under the code-name Echelon, it is unclear whether this was its official title or whether Echelon actually referred to a single project component. The programme was originally founded by the United States National Security Agency (NSA) and Great Britain's Government Communications Headquarters (GCHQ), with the construction of two ground stations to intercept satellite traffic. One station was located in Yakima, in the northwest United States, and the other was in Cornwall, England.

Over the following decades, the programme expanded significantly. Spy agencies in Australia, New Zealand and Canada joined the programme, and there were reports of collaboration with Denmark and Holland. Although the system was ostensibly targeted at the Soviet Union and its Eastern Bloc allies, it intercepted communications information indiscriminately, relying on automated **filters** to sort pertinent from non-pertinent data.

The Five Eyes

The "**Five Eyes**" is the name of a surveillance agreement established between the United States' NSA, Canada's Communications Security Establishment (CSE), the United Kingdom's GCHQ, Australia's Defence Signals Directorate (DSD) and New Zealand's Government Communications Security Bureau (GCSB). The collaboration grew out of the United Kingdom-United States of America Agreement (UKUSA), a multilateral treaty on sharing signal intelligence which was signed in 1946. It was later extended to include the other three partners.

Although initially a Cold War operation, Echelon later expanded significantly beyond the parameters of that conflict. For example, there have been accusations that Echelon was being used to perpetrate acts of **economic espionage**. The most notable case was in 1995, when a journalist from the *Baltimore Sun* claimed that the NSA had intercepted faxes and phone calls made between Airbus, a European aircraft manufacturer, and the Saudi government during competition for a USD6 billion contract.[1] The intercepted communications apparently revealed that Airbus was bribing Saudi officials, information which the United States used to ensure that the contract was awarded to Boeing Co. and MacDonnell Douglas Corp., two US companies. Although the USA officially denied involvement, James Woolsey, a former Director of the Central Intelligence Agency, responded to European complaints with an article acknowledging that the USA conducts economic espionage, but claiming that it was justified since European companies routinely used bribery to advance their interests.[2]

Although the Echelon system was[3] a powerful tool, it faced two major limitations. The first is that it relied heavily on intercepting **satellite** signals, which have never represented more than a small proportion of the total volume of communications. However, prior to the internet age, satellite communications were the only medium where pervasive surveillance was feasible.

Other types of surveillance required a far more distributed geographic presence, to intercept radio waves and tap thousands of individual cables. Although there is some evidence that Echelon included components aimed at gathering intelligence via these other media, in a pre-digital world pervasive data collection would have required an infrastructural presence that was beyond its capabilities, at least according to the European Parliament's 2001 *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system).*[4] An additional limit stemmed from the analytical resources available at the time. Although the information which was absorbed represented a small proportion of total communications on the planet, it nonetheless represented far more data than could be analysed effectively or even stored at the time.

THE INTERNET'S ROLE IN FACILITATING MASS SURVEILLANCE

There are several reasons why the internet has made pervasive data collection easier. One is that the internet has consolidated communications infrastructure. Traditional forms of communication are carried through individual and independent networks. The infrastructure for sending mail, for example, is completely different from the infrastructure for making a phone call. Monitoring a target's written communications and monitoring their phone lines required separate operations. Online communications, by contrast, consolidate different forms of communication (phone, email, video conferencing and so on) into a single data flow, making it much easier to harvest the information.

Online communications consolidate many different forms of communication into a single data flow, making it much easier to harvest the information

An additional advantage, at least for the United States, lies in the way internet communications travel. In contrast to a phone call or letter, information sent via the internet does not necessarily travel via a direct geographic route. Other considerations, notably cost, play a role in how information packets are sent. For example, a particular service provider may want to send information in a way that keeps it on a network that they control as far as possible, even if this means using a geographically circuitous route.

Because the United States hosts so much of the world's internet structure and so many major internet companies, a large amount of the world's web traffic flows through the United States, creating opportunities for interception. So, while a letter which was sent from Mexico to Spain would be unlikely to pass through the United States, an online communication between users in these countries almost certainly would.

"FIVE EYES" SURVEILLANCE SYSTEMS: WHAT WE KNOW

As of March 2014, only a small percentage of the Snowden leaks have been publicly released. Glenn Greenwald, Laura Poitras and other journalists continue to process their way through the enormous trove. It may be years before a complete picture of the leaked information emerges. Moreover, it is safe to assume that surveillance practices have already changed since the Snowden disclosures.

In part this may be attributed to expressions of outrage at particular policies. For example, following German complaints over revelations that the NSA had spied on their Chancellor, Angela Merkel, US President Barack Obama promised that Ms. Merkel would no longer be surveilled (although there have been reports that, after this directive was issued, the NSA sought to expand surveillance of Ms. Merkel's ministers to make up for the intelligence shortfall).[5] It is also possible that the **Five Eyes** partners will seek to alter their methods for operational reasons. Intelligence agencies involved in the programmes have repeatedly declared that Snowden's leaks compromised the efficacy of their tactics.[6] Although the veracity of these statements has been called into question, and some believe that the claims of harm are merely an attempt to undermine the argument that Snowden's leaks were in the public interest, it is reasonable to expect that the agencies involved were at least forced to re-evaluate their tactics as a result of the revelations.

Edward Snowden

A large amount of what we know about digital surveillance has been brought to light through the efforts of Edward Snowden, who at the time was a 29-year old infrastructure analyst employed by Booz Allen Hamilton Inc., a management consulting firm which had been hired by the NSA as an independent contractor.

Over the course of three months in 2013, Snowden downloaded an enormous volume of classified material about digital surveillance programmes being carried out by the NSA and its partners. He shared the documents with two journalists, Glenn Greenwald and Laura Poitras, before flying to Hong Kong to await the story's publication on 5 June.

It is impossible to overstate the impact of Snowden's revelations on the discourse about online surveillance and privacy. In the United States, there have been several legislative attempts to

curtail or reform the programme, as well as an external review of surveillance practices, although the announced changes have fallen far short of what civil society has been demanding. The revelations have prompted furious official responses from dozens of other countries, notably Germany, Indonesia and Brazil, whose leaders had all been targeted. Some governments have responded by proposing sweeping changes to the programmes while others have limited their complaints to the targeting of high-level victims.

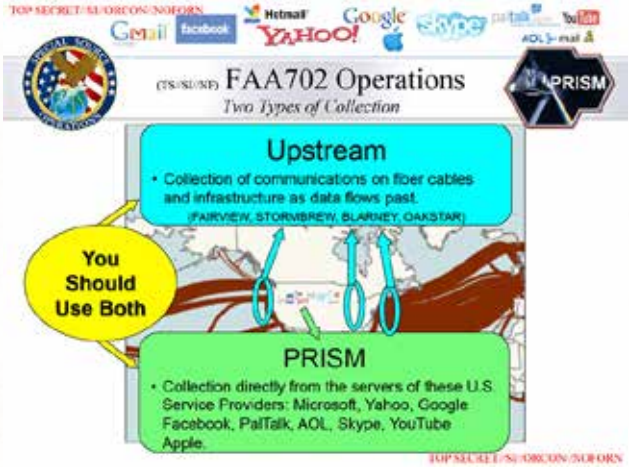
Snowden himself has faced enormous personal cost as a result of his actions. On June 14, he was charged in the United States with theft of government property as well as offences under the Espionage Act. His attempts to reach asylum in Latin America were stymied when the United States cancelled his passport en route, stranding him in Russia. The United States, with the help of the Spanish, Italian and French governments, even went so far as to force down the plane of Bolivia's President Evo Morales on 1 July 2013, out of concern that Snowden may have been on board. After spending over a month in the transit section of Moscow's Sheremetyevo Airport, Snowden was offered a year's temporary asylum in Russia, where he remains at the time of writing.

In the opinion of most human rights groups Edward Snowden is a whistleblower whose actions exposed wrongdoing and were clearly in the public interest. According to international human rights standards, whistleblowers should be protected from sanction as long as they act in good faith and with the reasonable belief that the information they disclose is substantially true and provides evidence of wrongdoing.

According to the Snowden revelations, there are two main ways in which the **Five Eyes** carry out surveillance: **upstream collection** and through the **PRISM** programme.

UPSTREAM COLLECTION

Upstream collection intercepts information that is being carried on **fibre-optic cables** and other infrastructure as it is in transit. So far, four programmes of this type have been identified, which are codenamed BLARNEY, FAIRVIEW, STORMBREW and OAKSTAR.[7]



This slide, from an NSA powerpoint presentation leaked by Edward Snowden, summarises the two major avenues used to harvest information.

Although the details remain murky, it is believed that **upstream collection** takes place with the cooperation of US-based telecoms companies through the installation of monitoring hardware at key chokepoints along the internet's backbone. Mark Klein, a former employee at AT&T, a major telecommunications provider, testified that in 2003 he witnessed the installation of splitting devices in the company's San Francisco office, which served as a hub for directing communications traffic to several internet networks and **internet exchange points** in the United States.[8] The splitting devices utilised

deep packet inspection (DPI) technology to duplicate information streams, sending the results to a secure room, to which access was restricted to representatives of the NSA. Mr. Klein further testified that conversations with other AT&T technicians revealed that similar "splitter cabinets" had been installed in San Jose, Seattle, Los Angeles and San Diego. It is believed that these mechanisms are part of Project BLARNEY, with AT&T as the "commercial partnership" referenced in the leaked slides. STORMBREW is thought to be a similar programme involving Verizon, another US-based carrier.

Tapping a Fibre-optic Cable

Fibre-optic cables (also known as optical fibre-cables) are the primary means of carrying information along the internet's main arteries. This is largely because of their fast data speeds and high carrying capacity. They also have low attenuation rates, meaning signals degrade very little over long distances.

Fibre-optic cables are comparatively difficult to monitor surreptitiously. Unlike copper wires, which can be tapped by observing the electro-magnetic field they generate, communications carried on fibre-optic cables can only be intercepted by physically cutting into the cable and diverting the signals into a separate bank. In order to intercept the information surreptitiously, a surveillance mechanism also needs to be capable of instantaneously reproducing the signals and sending them back along the line.

Deep Packet Inspection

DPI is a controversial technique which involves automatically examining all internet traffic in search of particular signatures, such as a keyword or a fragment of computer **source code**. While there are legitimate uses of DPI, such as to screen out **viruses** or defend against **distributed denial of service attacks**, its wholesale use is an extremely invasive form of surveillance. Moreover, a sophisticated DPI system can even be used to modify internet traffic on the fly, for example by deleting unfavourable references to a particular political leader on a website and replacing them with favourable ones, leaving the user unaware of the change.

As discussed earlier, the nature of the internet's infrastructure and the global prevalence of US-based services, such as Google and Facebook, allow these programmes to siphon an enormous amount of global information traffic, including data packets whose sender and recipient may not have any connection to the United States. According to some estimates, the NSA has access to 75% of the internet traffic which flows through the United States.[9] The NSA's reach is further expanded by the fact that the US-based interception points are complemented by a number of "foreign access points". It is important to note that this collection is not limited to **metadata**, but extends to the content of the communications themselves.

This system picks up far more data than can readily be analysed, including at least 1.7 billion emails per day, according to one estimate.[10] The NSA also faces legal constraints on its ability to monitor US citizens or residents. Consequently, several layers of **filtering** take place. First, the NSA instructs its telecoms partners only to send over information that pertains to certain "areas of interest", likely based on particular keywords or users. The NSA itself will then sift through the resulting information, deciding what to keep and what to discard. William Binney, a former NSA

employee, estimated that over an eleven year period the NSA has collected between 15 and 20 trillion transactions.[11]

Although this represents a relatively small proportion of total communications, it is worth noting that the NSA is dramatically expanding its data storage capacity with the recent construction of a USD2 billion data storage facility in Utah.[12]

According to some estimates, the NSA has access to 75% of the internet traffic which flows through the United States, a total of 1.7 billion emails per day.

PRISM

These data collection methods are complimented by a second programme, known by the code-name **PRISM**, which mines stored data from nine U.S. companies: Microsoft, Google, Yahoo, Facebook, PalTalk, AOL, Skype YouTube and Apple. As discussed in the introduction, these private companies store enormous amounts of information about their users, and also maintain access to their online messaging accounts. As of 5 April 2013, there were 117,675 active targets whose communications were being monitored under the PRISM programme.[13] The Snowden leaks suggest that the NSA enjoys direct access to the central **servers** of the nine companies, allowing them to harvest information about their targets at will.

Although it is clear that US-based telecoms, notably AT&T and Verizon, have been actively cooperating with the NSA's data collection activities, several of the companies listed under the **PRISM** programme have vociferously denied voluntary involvement or having given the NSA direct access to their central

servers. These companies are, however, legally prohibited from speaking openly about the nature of their cooperation. Google, Microsoft and Yahoo have filed suits against the NSA to allow them to disclose more information about their role in the programme.[14]

Legally, the companies are required to comply with specific NSA requests. However, the Snowden revelations make it clear that the NSA faced differing levels of resistance from them. The leaks describe Microsoft as becoming **PRISM**'s first "corporate partner", in May 2007. Apple did not join the programme for another five years. Dropbox, a company which provides cloud storage services, is listed in one slide as "coming soon", while Twitter is not listed as a partner. Suspicion of Apple's role in actively facilitating the surveillance also stems from a leaked presentation, dated October 2008, which described a **software** implant called DROPOUT JEEP that had a claimed 100% success rate for **hacking iOS** devices. The **virus** allowed for total control over an infected machine, including the ability to remotely activate the microphone and camera. Given the claims of perfect success, some experts have expressed scepticism that the **exploit** could have been designed without Apple's cooperation.[15] In other words, there is suspicion that Apple provided the NSA with a **backdoor** to access its products, although Apple strongly denies this.[16] AOL, PalTalk and Facebook have also denied participation in the PRISM surveillance programmes.[17] However, in March 2014 the NSA's General Counsel testified that both the PRISM and upstream data collection programmes took place with the "full knowledge and assistance" of the companies involved.[18]

Against the backdrop of corporate denials, it is also worth noting that a senior Verizon executive, John Stratton, specifically came out in support of the NSA surveillance, and criticised the objections that other tech companies had voiced:

> *This is a more important issue than that which is generated in a press release. This is a matter of national security… As it relates to the NSA — as has been discussed, the information was conveyed under a very rigorous process that had oversight by all three branches of the United States government.*[19]

Although these programmes give the NSA access to an enormous volume of data, the agency and its allies face an additional challenge in that much of the information they are interested in is **encrypted**. Although modern encryption methods are incredibly powerful, the Snowden leaks describe a massive programme, with funding of over USD250 million per year, aimed at penetrating encryption techniques. One major element of the programme involves inserting **backdoors** into commonly used encryption standards. For example, the NSA apparently paid RSA Security, a respected encryption company, to include a weak **algorithm** in a security enhancement program called Bsafe (RSA has denied the allegations that they deliberately weakened the product at the request of the NSA).[20] In interviews, Edward Snowden reported that strong encryption tools, when used properly, remain effective. However, his leaked documents revealed the existence of an USD80 million project to build a **quantum supercomputer** capable of cracking even advanced encryption standards.[21]

Tor, a popular tool designed to protect online **anonymity**, was also a major target of the NSA. However, the Snowden leaks indicate that the agency was unable to substantially crack the system. One presentation, tellingly entitled "Tor Stinks", noted that the NSA was only able to de-anonymise "a very small fraction" of Tor users.[22] The NSA's frustration with Tor is ironic given that Tor's work was originally sponsored by the US Naval Research Laboratory and that the US government remains a major funder.

DOMESTIC SURVEILLANCE PRACTICES

Cooperation with the Five Eyes

Among European States, surveillance activities are sometimes boosted through collaborative agreements with the **Five Eyes**. In his testimony to the European Parliament on 7 March, 2014, Edward Snowden noted:

> *The best testimony I can provide on this matter without pre-empting the work of journalists is to point to the indications that the NSA not only enables and guides, but shares some mass surveillance systems and technologies with the agencies of EU member states. As it pertains to the issue of mass surveillance, the difference between, for example, the NSA and FRA [Sweden's National Defence Radio Establishment] is not one of technology, but rather funding and manpower. Technology is agnostic of nationality, and the flag on the pole outside of the building makes systems of mass surveillance no more or less effective.*[23]

Snowden's testimony also noted that the NSA and the GCHQ employ lawyers to search for loopholes in their allies' legal or constitutional privacy and due process protections, and then offer these novel interpretations as "legal guidance" in support of cooperation on indiscriminate surveillance matters. Another interesting note in Snowden's testimony is that **Five Eyes** collaboration with European nations frequently includes the caveat that the espionage must not target citizens of the collaborating State, although this limitation is easily sidestepped:

> *The result is a European bazaar, where an EU member state like Denmark may give the NSA access to a tapping center on the (unenforceable) condition that NSA doesn't search it for Danes, and Germany may give the NSA access to another on the condition that it doesn't search for Germans. Yet the two tapping sites may be two points on the same cable, so the NSA simply captures the communications of the German citizens as they transit Denmark, and the Danish citizens as they transit Germany, all the while considering it entirely in accordance with their agreements.*
>
> *Ultimately, each EU national government's spy services are independently hawking domestic accesses to the NSA, GCHQ, FRA, and the like without having any awareness of how their individual contribution is enabling the greater patchwork of mass surveillance against ordinary citizens as a whole.*

Other countries' surveillance programmes

The **Five Eyes** operate what is likely the world's most advanced and pervasive global surveillance apparatus. Partly this is due to the "home field advantage" that the United States enjoys since it hosts much of the internet's architecture and many leading global technology companies. The Five Eyes also operate at a level that is beyond the capabilities of most, if not all, other powers, with regard to both their global presence and the information processing power they are able to bring to bear. However, while pervasive global surveillance requires a global presence, pervasive domestic surveillance does not. A State which is able to exercise control over its domestic internet infrastructure can monitor the communications of its residents.

Outside of the developed democracies, governments are generally far more interested in using the internet to monitor their own people than as a tool for external surveillance. Although details are sketchy, Russia appears to be in the process of instituting an extremely invasive programme of internet censorship, including extensive surveillance policies. These are being introduced as a means of implementing a law passed in July 2012, On amendments to the Federal Statute 'On the Protection of Minors against Information Detrimental to their Health and Development' and to other legal Acts of the Russian Federation (the Amendments), which has drawn international condemnation for its prohibition of material which "propagandises non-traditional sexual relations".[24]

Sources have indicated that the Russian government plans to enforce these content controls online through the installation of DPI systems at every **internet service provider** (ISP). In April 2014, Russian President Vladimir Putin strongly denied that an invasive surveillance programme was in place, although his claims were met with broad scepticism.[25]

Several other countries have introduced DPI with the partial aim of blocking anonymisation **software**, including Ethiopia,[26] Iran[27] and Kazakhstan.[28] It is worth noting that **Tor** has come up with their own workarounds to evade some of these blocking systems.

Intensive surveillance programmes are also part of China's extensive apparatus for controlling the internet. Several government departments include surveillance of the web within their mandates, described by euphemisms such as "the study of public opinions".[29] China's surveillance system also includes extensive cooperation with the private sector, including through the installation of DPI systems and mechanisms which automatically block the transmission of **encrypted** content. Beyond cooperating with State surveillance bodies, companies operating in China are often legally responsible for keeping an eye on their users.

Companies operating in China are often legally responsible for keeping an eye on their users.

Sina Weibo, China's version of Facebook/Twitter and one of its most popular websites, now requires users to register using their real names and telephone numbers. The website also operates a demerit system, whereby breaches of the terms and conditions lead to deductions. Running out of points will lead to an account's deletion. Users running low on points can recover them through good behaviour for a period of time or through performing an unspecified "promotional activity".[30]

As a result of these requirements, Chinese companies have developed into world leaders in facilitating online surveillance. In 2012, ZTE Corp, China's second-largest telecommunications maker, came under fire for selling powerful surveillance equipment to Iran. Because this sale may have included embargoed U.S. equipment, ZTE Corp ended up selling the subsidiary which manufactured the system.[31] ZTE Corp's internet surveillance equipment was also found in Libya after the fall of Muammar Gaddafi's dictatorial government in 2011.[32]

The role of western technology

Western companies also play a key role in facilitating domestic surveillance of the internet, including by repressive governments. For example, Trovicor, which manufactures the most widely used online surveillance system in the world, is based in Germany and was formerly a subsidiary of Nokia Siemens. A company brochure from 2007 stated that its monitoring systems had been installed in 60 countries, including Syria, Yemen, Egypt, Bahrain and Iran.[33] In 2009, due to pressure following Iran's violent crackdown on protestors, Nokia Siemens sold Trovicor. Trovicor continues to work with the Iranian government under its new owners, the German-based Perusa Partners Fund.[34]

Blue Coat, which is based in the United States, is a major supplier of DPI systems. Although their products can be used for legitimate **network management** functions, they can also be used to intercept and analyse traffic, including **encrypted** traffic. A study by the University of Toronto's Citizen Lab found indications that these systems were being used in Egypt, Kuwait, Qatar, Saudi Arabia, the United Arab Emirates, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey and Venezuela.[35] In response to inquiries made by Reporters Without Borders, Blue Coat said that the "misuse of technology to suppress freedom of expression or human rights was a serious issue, but not one that a single company could solve by itself".[36] It also referred to its "Ethics Policy for Partners" which, as of April 2014, makes no mention of human rights.[37]

Another widely used surveillance technology is the FinFisher Suite sold by Gamma International, a UK-based company. This product is more targeted, and operates through **malicious software** installed on a particular machine. A study by Citizen Lab found evidence that FinFisher is being used in Australia, Austria, Bahrain, Bangladesh, Brunei, Bulgaria, Canada, Czech Republic, Estonia, Ethiopia, Germany, Hungary, India, Indonesia,

Japan, Latvia, Lithuania, Macedonia, Malaysia, Mexico, Mongolia, Netherlands, Nigeria, Pakistan, Panama, Qatar, Romania, Serbia, Singapore, South Africa, Turkey, Turkmenistan, United Arab Emirates, the UK, the USA and Vietnam.[38]

DATA RETENTION OBLIGATIONS

Another common channel for surveillance is through **data retention** obligations. These systems effectively allow law enforcement to piggyback off of the information gathering abilities of private telecommunications and **ISPs**, rather than being required to collect the data themselves. As mentioned in the introduction, data collection for advertising purposes is a major part of many companies' business models while for others it is inherent in the services which they provide.[39] A data retention obligation requires companies to collect and store certain categories of information for a particular period of time, disclosing it to law enforcement upon request (a warrant or some other form of procedure may be required).

The chief difference between **data retention** schemes and blanket State surveillance mechanisms such as the NSA's Upstream programme is that, for the most part, the information collected under a data retention directive remains in the hands of private companies, rather than State agencies. Although the companies involved collect the information indiscriminately and in bulk, State access to that information requires State actors to go through some sort of procedure so that access is generally more targeted. As a result, data retention is normally less intrusive. However, it is important to note that data retention schemes and blanket State surveillance mechanisms are not mutually exclusive. For example, Russia and China both have data retention requirements in place.[40]

European Data Retention Directive

The most prominent of these systems was the EU's 2006/24/EC (the **Data Retention** Directive), which obliged all EU States to pass legislation requiring service providers to retain the traffic and location data of all users' telephone and internet communications for between six months and two years.

The EU Data Retention Directive, which has been struck down as an invasion of privacy, was far less intrusive than the Five Eyes programme

From the start, the **Data Retention** Directive was highly controversial. Several EU States refused to implement it, including Germany and Sweden, and courts in the Czech Republic, Cyprus, Bulgaria and Romania held that its provisions were unconstitutional. In April 2014, in response to a challenge brought by Digital Rights Ireland, the European Court of Justice (ECJ) invalidated the Data Retention Directive, ruling that it was incompatible with the privacy and data protection provisions of the Charter of Fundamental Rights of the European Union.[41] In particular, the ECJ found that the Data Retention Directive was disproportionately invasive, noting that it applied to all electronic communications of all persons, that there were insufficient limits on access and use of the data by law enforcement, and that the retention period of at least six months was too long.[42] The ECJ also noted that, since some of the service providers impacted by the Data Retention Directive were located outside of the EU, there was no way to ensure that the stored data would be safeguarded appropriately.

Given the ECJ's finding, it is worth noting that the **Data Retention** Directive is far less intrusive than the **Five Eyes** programme, with which many European States are known to have collaborated. The Data Retention Directive only applies to traffic information and **metadata**, and does not include the content of messages. Additionally, rather than being collected and warehoused by the State, the Data Retention Directive keeps this information in the hands of the service providers. Law enforcement authorities are only allowed to access this information as part of a targeted investigation of "serious crimes" rather than carrying out blanket monitoring.

National data retention regimes

Data retention schemes exist in several countries. In Thailand, the Thailand Computer Crime Act, B.E. 2550[43] requires **ISP**s to archive identifiable computer traffic data for at least 90 days, with steep fines for either failing to retain the data or failing to present it to authorities upon request. It is worth noting that the Act also contains several cyber offences which are illegitimate according to international human rights standards, for example it has frequently been used to target internet users deemed to have insulted Thailand's King.[44]

India also has a **data retention** scheme, based on licensing requirements for **ISPs** and unified access service providers contained in the Indian Telegraph Act, 1885. Their licences require ISPs to retain "all commercial records with regard to the communications exchanged on the network" for a period of at least one year. The Information Technology (Amendment) Act, 2008[45] also contains data retention requirements.

The Philippines' Cybercrime Prevention Act of 2012 contains a **data retention** scheme which requires service providers to build a database of information about their subscribers by recording all traffic and content information and the identity behind each **IP**

address, and to preserve this information for at least six months, and for an additional six months when specifically requested to do so by law enforcement officials.[46] Law enforcement officials require a court warrant to access this subscriber information. However, the Act allowed authorities to monitor traffic data (not including content) without the need for a warrant, requiring only "due cause". The Act faced significant opposition, including a judicial challenge. In February 2014, the Philippines' Supreme Court ruled that the provision granting law enforcement officials the power to record traffic data without a warrant was unconstitutional, although most of the rest of the Act was upheld.[47]

KNOWN ABUSES OF SURVEILLANCE SYSTEMS

As discussed in Chapter 2, an overly intrusive approach to surveillance is, by its very nature, abusive. However, before moving on, it is worth noting a few specific examples of abusive conduct which illustrate the dangers inherent in granting spy agencies unduly broad powers of surveillance.

One disturbing, if entirely predictable, example is referred to inside the NSA as LOVEINT. In response to an inquiry about whether there had been specific cases of NSA officers abusing their powers, NSA Inspector General George Ellard responded by detailing several cases of agents who had spied on current or former partners or spouses.[48] In some instances, the searches were specifically designed to investigate whether the person had been unfaithful, while in others they were claimed to have been done for "practice".

An even more disturbing invasion of privacy was uncovered in February 2014, when it was announced that the GCHQ had collected and stored webcam images from millions of randomly selected Yahoo users. The intercepted communications included

enormous volumes of sexually explicit imagery, estimated as being between 3% and 11% of the total.[49]

There is also evidence that the **Five Eyes** spying programme has gone beyond its national security mandate to carry out **economic espionage**, for example by spying on Petrobras, a large Brazilian oil company, as well as other targets in that country's mining and energy industry.[50] More recently, there have been allegations that the Five Eyes mechanisms were used to monitor the communications of **Kim Dotcom**, a businessman.[51] Diana Spencer, Princess of Wales, was another reported target of the Five Eyes programme.[52]

Internet surveillance techniques are deployed against journalists, dissidents and other political opponents

Internet surveillance techniques are deployed extensively against journalists, dissidents and other political opponents. For example, in 2013 the Russian government passed a special decree authorising digital surveillance practices at the 2014 Winter Olympics in Sochi which explicitly named journalists and foreign media organisations as targets.[53] Many Arab governments employed internet surveillance techniques to combat the wave of protests that spread across the region in 2011. For example, authorities in Bahrain interrogated human rights activists and journalists using transcripts of electronic communications obtained through their pervasive surveillance mechanisms. Many of the victims were also tortured, and several have been convicted and sentenced to long prison terms.[54]

Surveillance mechanisms can transform the internet into a tool for control. Some observers were surprised when, in February 2011, the Syrian government suddenly reversed a long-standing

ban on social media sites including Facebook, Twitter and YouTube. However, their rationale for relaxing restrictions in the face of regional unrest was to encourage protesters to use means of communication which the authorities could monitor. As the Syrian protests spread, information gathered through online surveillance played a key role in the arrest and torture of dissidents.[55]

In 2012, Ai Weiwei, a prominent Chinese dissident, mocked the ongoing surveillance against him by setting up webcams in his office and bedroom to provide his own continuous live webfeed, although the website was shut down almost immediately by the Chinese authorities.

Although the targeting of journalists and activists is most acute in the developing world, there have been allegations that the **Five Eyes** programme targeted human rights organisations such as Amnesty International and Human Rights Watch.[56] There are also indications that the NSA's surveillance apparatus, along with the Obama administration's zealousness in prosecuting whistleblowers, has chilled the ability of journalists to speak to sources in the United States. According to a report on shifting attitudes, one journalist was quoted as saying:

> *I worry now about calling somebody because the contact can be found out through a check of phone records or e-mails… It leaves a digital trail that makes it easier for the government to monitor those contacts.*[57]

Another journalist in the same report said:

> *There is greater concern that their communications are being monitored—office phones, e-mail systems. I have to resort to personal e-mail or face to face, even for things I would consider routine.*

CHAPTER 2:

INTERNATIONAL HUMAN RIGHTS STANDARDS AND DIGITAL SURVEILLANCE

International Human Rights Standards And Digital Surveillance

THE RIGHT TO PRIVACY

The debate about mass surveillance of the internet engages fundamental human rights, most obviously the right to privacy, which is critical to human dignity and individual autonomy. The ability to maintain privacy is important to both social interactions and interactions with the State. Although privacy is difficult to define comprehensively, it is recognised that it covers communications as well as other matters in relation to which people have a reasonable expectation of privacy.[58]

International Human Rights Law

The cornerstone of modern human rights is the *Universal Declaration of Human Rights* (UDHR), which was adopted as a resolution of the UN General Assembly in 1948. Although UN resolutions are generally not legally binding on States, at least parts of the UDHR are broadly recognised as having gained legal force as customary international law, with the result that they are legally binding on all States. The rights contained within the UDHR were enshrined in two international conventions which were drawn up in 1966: the *International Covenant on Civil and Political Rights* (ICCPR) and the *International Covenant on Economic, Social and Cultural Rights*. Similar standards are also reflected in several regional human rights treaties.

The importance of the right to privacy is recognised in the *Universal Declaration of Human Rights* (UDHR):

> *Article 12*
>
> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*[59]

Parts of the UDHR, including the right to privacy, are broadly accepted as constituting customary international law, meaning that they are legally binding on all States. The right to privacy is also guaranteed by the International Covenant on Civil and Political Rights (ICCPR):

> *Article 17*
>
> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks.*[60]

Customary International Law

In contrast to treaties, which are only binding on those States that chose to ratify them, customary international law, which arises from established State practice, is universally binding. The basic idea here is that some principles are so universally recognised that, even in the absence of a specific treaty or other written statement, they may be considered to be binding upon all States.

A good example of customary international law is the rules pertaining to the seas, especially before they were codified in 1982 in the Convention on the Law of the Sea. Prior to that, rules relating to economic exploitation of the seas, travel and so on, which were central to important parts of human commerce, were all widely respected as matters of customary international law.

As of March 2014, there were 167 State parties to the ICCPR, including all of the **Five Eyes** countries. The right to privacy is also recognised in over 100 national constitutions, as well as in regional human rights instruments, which are legally binding on their signatories. For example, the *American Convention on Human Rights* states:

> *Article 11. Right to Privacy*
>
> *1. Everyone has the right to have his honor respected and his dignity recognized.*
>
> *2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.*
>
> *3. Everyone has the right to the protection of the law against such interference or attacks.*[61]

The European Convention on Human Rights protects the right to privacy along similar lines:

> *Article 8 – Right to respect for private and family life*
>
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The European Court of Human Rights (ECHR), the international body charged with interpreting the *European Convention on Human Rights*, has set out a relatively clear approach to assessing the legitimacy of interferences with the right to privacy in its case law. In order to be legitimate, an interference must be authorised by law and be carried out in accordance with that law. It must also be necessary in a democratic society which means, among other things, that the interference corresponds to a pressing social need and is proportionate to the legitimate aim pursued.

Currently, there is a case before the ECHR which alleges that the UK's role in the **Five Eyes** surveillance programme is a violation of Article 8, guaranteeing privacy.[62]

In previous cases, the ECHR has stressed that surveillance programmes must strictly meet the requirement that interferences with privacy should be "in accordance with the law". This means, among other things, that the legal rules authorising surveillance activities should be accessible and make clear the circumstances in which surveillance might be engaged:

> *[T]here must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident… the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.*[63]

Given their nature, it is hard to believe that the Court will accept that the legal basis for the surveillance programmes revealed by Snowden meets the standard of being accessible and foreseeable. This is corroborated by the scale and nature of the reaction to the revelations, in the UK as elsewhere, which demonstrates that even careful security watchers were not aware that these activities were taking place, let alone that they were foreseeable. It is also worth noting that the Regulatory of Investigatory Power Act 2000, from which the GCHQ derives its surveillance powers, is notoriously broad and flexible, which is exactly the sort of provision that the European Court might find fails to meet the required standard of being "in accordance with the law".[64]

At the same time, the ECHR has tended to give States some latitude in determining whether their national security programmes meet the standards of necessity and proportionality:

> *By reason of their direct and continuous contact with the pressing needs of the moment, the national authorities are in principle in a better position than the international judge to decide both on the presence of such an emergency and on the nature and scope of derogations necessary to avert it.*[65]

It is important to note that, although the ECHR has relatively well-developed standards regarding privacy, international standards in this area are significantly less developed, and the legal provisions are correspondingly less clear.

PRIVACY AND FREEDOM OF EXPRESSION

In addition to its importance as a human right, privacy is vital for the fulfilment of other fundamental human rights, notably the right to freedom of expression. Control over one's communications, including over who has access to them, is a key element of expression. Studies have shown that perceptions of control lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.[66] The nexus between privacy and freedom of expression has been noted by the UN Special Rapporteur on Freedom of Opinion and Expression:

> *States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy.... Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.*[67]

The importance of **anonymity** to online expression was also recognised in the Council of Europe Declaration on Freedom of Communication:

> *In order to ensure protection against online surveillance and to enhance the free expression of information and ideas (...) States should respect the will of users of the Internet not to disclose their identity.*[68]

Perceptions of control lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.

In this context, it is important to note that not only laws but also policies and even indirect actions which exert a **chilling effect** on free speech represent interferences with freedom of expression. This is explicitly recognised in Article 13(3) of the *American Convention on Human Rights*:

> *The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.*[69]

The link to freedom of expression, which is particularly relevant in the context of surveillance of communications data, is important because the test for restrictions on freedom of expression under international law is clear and well established, and requires States to meet a similar three-part test to that applied by the European Court in the context of privacy. First, the restriction must be provided by law or imposed in conformity with the law, which is arguably similar to the requirement of legality for restrictions on privacy in Article 17 of the ICCPR. Second, the restriction must pursue one of the legitimate aims listed in Article 19(3) of the ICCPR, namely respect for the rights and reputations of others, or the protection of national security, public order (ordre public), or public health or morals. Third, the restriction must be necessary to secure the aim, which also incorporates a proportionality element.

HUMAN RIGHTS AND THE INTERNET

With the rise of the internet, the application of human rights, including the right to privacy, to digital contexts is increasingly being explicitly affirmed, although it also flows naturally from general principles of human rights law. For example, in June 2012, the UN Human Rights Council stated: "[T]he same rights that people have offline must also be protected online, in particular freedom of expression".[70] The UN General Assembly adopted a resolution in November 2013, which similarly affirmed "that the same rights that people have offline must also be protected online, including the right to privacy".[71]

In the context of surveillance, the expansion of the internet and digital communications has been a game-changer. This was recognised as early as 2002 in the Inter-American Commission on Human Rights' *Report on Terrorism and Human Rights*:

> *Advances in modern technology have rendered certain forms of communication, such as cellular telephones and electronic mail, particularly susceptible to improper surveillance by state authorities. It has been recognized in this regard that individuals may have vital privacy interests in personal information gathered by the state concerning their status or activities. States are therefore required to conduct their initiatives in this regard in compliance with prevailing norms and principles governing the right to privacy. This encompasses ensuring that the collection and use of personal information, including any limitations upon the right of the person concerned to access that information, is clearly authorized by law so as to protect the person concerned against arbitrary or abusive interference with privacy interests, and accordingly that judicial supervision is available to guard against abuses of these legal requirements. [references omitted]*[72]

Martin Scheinin, formerly the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, noted in his 2009 report that the right to privacy was being violated by ongoing signal intelligence collection efforts.[73]

In his 2013 report, Frank la Rue, United Nations Special Rapporteur on the promotion and protection of freedom of expression and opinion noted:

> *Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression.*[74]

Public concern about this issue has increased significantly in the aftermath of the Snowden revelations. In June 2013, two international rapporteurs on freedom of expression – at the United Nations (UN) and the Organization of American States (OAS) – issued a Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression.[75] The Joint Declaration noted that, while the protection of national security could in exceptional cases justify the surveillance of private communications, "given the dynamic character of the Internet and of communications technology in general, this type of surveillance may constitute a particularly invasive act that seriously affects the right to privacy and freedom of thought and expression." The Joint Declaration also noted a pressing need for new regulations to govern the digital surveillance programmes which are operated by law enforcement agencies in countries around the world. The Declaration specifically called for these programmes to be subject to due process guarantees and judicial oversight, and to respect the principle of proportionality.

Navi Pillay, the UN High Commissioner for Human Rights, has also warned of the human rights implications of mass surveillance programmes, and noted that States needed to update their legislation to take into account changes to the surveillance landscape brought about digitisation.[76] Ms. Pillay has also noted:

> *Modern technologies are transforming the way we do human rights work. In 1993, the World Wide Web was just four years old, and its future use and reach could barely have been imagined, nor how fundamentally the Internet would affect our lives. Together with social media and IT innovations, these technologies are dramatically*

> *improving real-time communications and information-sharing. They are also magnifying the voice of human rights defenders, shining a light on abuses, and mobilizing support for various causes in many parts of the world.*
>
> *But we have also seen how new technologies are facilitating the violation of human rights, with chilling 21st Century efficiency. In breach of international law, mass electronic surveillance and data collection are threatening both individual rights, and the free functioning of a vibrant civil society.*[77]

Around the world, civil society has also been highly vocal about the problems with mass surveillance. Among the most prominent campaigns has been the International Principles on the Application of Human Rights to Communications Surveillance (the International Principles).[78] Although these principles are not legally binding per se, they are significant inasmuch as they help contribute to the development of international human rights standards.

International standards relating to restrictions on privacy are relatively sparse, but there is a robust test for interferences with freedom of expression which can be readily applied to surveillance.

The fact that digital surveillance programmes have elicited such a negative reaction from across the human rights community strongly suggests that there is a serious problem with how these activities are being carried out. At the same time, international standards relating to restrictions on privacy as protected in Article 17 of the ICCPR are relatively sparse. There is, however, a

robust test for interferences with freedom of expression and, as noted above, it is firmly established that surveillance constitutes a dual interference with privacy and freedom of expression.

By considering the issue from a freedom of expression perspective, it is possible to arrive at a set of international standards for assessing whether a surveillance framework is legitimate. At the core of this are the requirements that any surveillance framework be clearly enumerated in law, pursue a legitimate aim, and be necessary and proportional to the achievement of that aim. The following section discusses the practical implications of this standard.

STANDARDS FOR LEGITIMATE SURVEILLANCE: CLEAR LEGAL DEFINITIONS

The first key principle is to ensure that the parameters governing surveillance activities are clearly spelled out in law. This derives directly from the requirement that restrictions on both privacy and freedom of expression must be "in accordance with the law" or "provided by law". This requirement implies not only that there is a legal rule justifying the restriction, but also that the legal rule is clear and accessible. Vaguely drafted restrictions may be interpreted in a range of different ways, which gives the authorities an unacceptable level of discretion in applying the rules and which may lead to applications of the restriction which do not correspond to the intended purpose of the authorising rule or to the legitimate aim sought to be protected. Vague rules also fail to give those subject to the law adequate notice of when the rule may be acted on (i.e. surveillance commenced). As a result, they exert an unacceptable **chilling effect** on privacy and freedom of expression as individuals steer well clear of the potential zone of application to avoid censure. As the Human Rights Committee has stated, in a General Comment on freedom of expression:

> *For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.*[79]

In the digital era, it is not enough to rely on rules designed for an offline world. As the June 2013 Joint Declaration of the special rapporteurs on freedom of expression makes clear, the changes wrought by digitalisation mean that new rules need to be adopted which are tailored to the new surveillance possibilities that have been created.

There are, of course, legitimate operational reasons why the specifics about a particular ongoing surveillance activity cannot be made public, but this is not the same as secrecy around the legal framework for such actions. Absent clear rules, those tasked with conducting surveillance will naturally tend to expand the scope of their operations and powers. To meet these conditions, any law authorising surveillance should detail the circumstances in which surveillance activities may be undertaken, i.e. what triggers the power of an agency to initiate a surveillance activity, the required conditions for authorisation of that activity, and exactly what can and cannot be done in the context of a surveillance operation.

These standards are reflected in Principle 10E of the *Tshwane Principles on National Security and the* ***Right to Information***, the leading statement on how to balance national security needs with transparency. The Principles were drafted by a broad coalition of civil society and academic experts and have been endorsed by the four special international mandates on freedom of expression (at the UN, the OAS, the OSCE and the ACHPR). The first clause of Principle 10E. Surveillance, states:

> *(1) The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.*

This principle is also reflected in paragraph 8 of the Joint Declaration by the special rapporteurs, which states:

> *In keeping with this, states must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged.*

Legislation which enables surveillance should also define clearly the scope of activities which are covered. For example, Section 4 of the Australian Security Intelligence Organisation Act 1979, defines "security" as:

> *(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:*
>
> *(i) espionage;*
>
> *(ii) sabotage;*
>
> *(iii) politically motivated violence;*
>
> *(iv) promotion of communal violence;*
>
> *(v) attacks on Australia's defence system; or*
>
> *(vi) acts of foreign interference;*
>
> *whether directed from, or committed within, Australia or not; and*
>
> *(aa) the protection of Australia's territorial and border integrity from serious threats; and*
>
> *(b) the carrying out of Australia's responsibilities to any*

> *foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).*[80]

This clear definition ensures that surveillance activities by the Security Intelligence Organisation are authorised only in relation to genuine national security matters, fulfilling the requirement that restrictions on privacy and freedom of expression pursue a legitimate aim.

As much information as possible about the powers of an agency which conducts surveillance should be set out in its enabling legislation.

A clear statement of purpose also helps to combat the threat of "mission creep", a natural tendency to expand the purview of a powerful agency or programme. The apparent use of **Five Eyes** resources to investigate **Kim Dotcom** for copyright offences and to carry out acts of **economic espionage**, are examples of this. Likewise, there is no conceivable national security justification for monitoring Human Rights Watch or Amnesty International.

Beyond a clear definition as to the scope of operations, as much information as possible about the powers of an agency which conducts surveillance should be set out in its enabling legislation. For example, Articles 25-37 of the *Act on the Security Intelligence System of the Republic of Croatia* contain a reasonably detailed description of the agency's powers and competencies.[81]

Better practice is also to subject surveillance activities to a general duty to protect human rights. For example, Brazil's Law 9,883 states that the "Brazilian Intelligence System is founded on the preservation of national sovereignty, the defense of the

democratic rule of law and human dignity, and shall comply with and preserve the individual rights and guarantees and other provisions of the Federal Constitution, treaties, conventions, international agreements and adjustments in the Federative Republic of Brazil is a party or signatory, and ordinary legislation."[82]

STANDARDS FOR LEGITIMATE SURVEILLANCE: TRANSPARENCY AND THE RIGHT TO INFORMATION

There is unquestionably a legitimate need to maintain some secrecy in relation to surveillance activities. It would, for example, clearly be unreasonable to expect surveillance agencies to release the names of active surveillance targets. At the same time, in order to facilitate a robust public debate on whether the authorities have struck an appropriate balance between privacy and security, clear legal rules must be accompanied by transparency in their application. Although the Snowden leaks have been widely criticised by the intelligence establishment, the journalists involved have carefully vetted the information that has been released, taking into account its potential to harm the ability of the agencies in question to operate. This is part of the reason why the revelations are being released at a relatively slow pace.

Clear legal rules must be accompanied by transparency in their application.

This is clearly reflected in the *Tshwane Principles on National Security and the* ***Right to Information***:

> *Principle 10E. Surveillance*
>
> *…*
>
> *(2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.*
>
> *(3) In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.*
>
> *(4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.*
>
> *(5) The high presumptions in favor of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.*

In other words, while it may be legitimate to withhold information about specific cases or investigations, information about bodies that conduct surveillance activities, along with statistical or aggregated information about those activities such as the total number of surveillance targets, should be made available. It is important to publish information about a surveillance organisation's hierarchy, structure and decision-making apparatus, including the results of any assessments as to the privacy or human rights implications of their work. Although there may be a need to redact certain information within these documents, severing out specific sentences or names should be seen as preferable to withholding entire documents. As with other organs of government, good practice also mandates the publication of completed access to information requests and detailed budget information.

The *Tshwane Principles* particularly emphasise the importance of maximum disclosure in relation to any illegal surveillance, reflecting the heightened public interest in rooting out abusive behaviour.

The Joint Declaration by the special rapporteurs also addresses the issue of transparency, stating, in paragraph 12:

> *... states should, at the very least, make public information regarding the regulatory framework of surveillance programs; the entities in charge of their implementation and oversight; the procedures for authorizing, choosing targets, and using the data collected; and the use of these techniques, including aggregate information on their scope.*

The need for disclosure of information which would not directly undermine the objectives of surveillance activities also flows from the **right to information** (RTI), a human right which is derived from the right to freedom of expression.[83] Core RTI principles establish a presumption in favour of the release of all information held by public authorities. As organs of the State, all intelligence agencies should be subject to RTI obligations, as should independent contractors retained to fulfil intelligence functions. For example, Rwanda's Law N° 04/2013 Relating to Access to Information applies to all public authorities, defined as:

> *Article 2(5)*
>
> *public organ: administrative entity established by the Constitution or any other Laws or any other organ that uses money from the national budget or any money originating from tax revenues as provided by the Law;*[84]
>
> *Similarly, Slovenia's Access to Public Information Act provides:*
>
> *Art 1(1)*
>
> *This Act governs the procedure which ensures everyone free access to and re-use of public information held by state bodies, local government bodies, public agencies, public funds and other entities of public law, public powers holders and public service contractors (hereinafter referred to as "the bodies").*[85]

This right of access should be limited only to protect recognised interests, which do include national security. However, international standards mandate that information should only be withheld if its disclosure would cause substantial harm to a protected interest, and that harm is greater than the public interest in disclosure. A good example of this balance can be found in Nicaragua's Law on Access to Public Information:

> *Article 7*
>
> *Principle of a harm test:*
>
> *Guarantees that the authority to determine that information is restricted must be based on and motivated by the following elements:*
>
> *a) The information must fall within a recognised exception spelled out in this law*
>
> *b) The release of the information will harm the public protected interest in the law.*
>
> *c) The harm that could result from the release of the information is greater than the public interest in knowing the relevant information.*[86]

This suggests that information about a surveillance action should normally be provided after it is finished and that any refusal to provide such information would be difficult to justify.

Where human rights have been or are being infringed, there is a very high public interest in favour of releasing relevant information. As Principle 10A(1) of the Tshwane Principles states:

> *There is an overriding public interest in disclosure of information regarding gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security. Such information may not be withheld on national security grounds in any circumstances.*

STANDARDS FOR LEGITIMATE SURVEILLANCE: OVERSIGHT

Proper oversight is necessary wherever State power is exercised and this is particularly important where human rights are being restricted. As Navi Pillay, the UN High Commissioner for Human Rights, put it, "internal safeguards without independent, external monitoring are ineffective against the abuse of surveillance methods."[87]

The need for independent institutional oversight over surveillance activities is reinforced by the fact that surveillance, almost by definition, takes place in secret and that there are, as a result, limitations on what information can be made public. As paragraph 9 of the Joint Declaration of the special rapporteurs notes, in part:

> *The collection of this information shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.*

Since a core goal of oversight is to ensure accountability, it is vital that the mechanisms of oversight should be precisely spelled out in law. There should be a clear chain of oversight linking the agents carrying out the surveillance to elected representatives in order to avoid plausible deniability if widespread abuses take place. A good example here is Article 11 of Hungary's Act 125 of 1995 on the National Security Services, which spells out the oversight duties of the Minister of National Defence.[88] Similarly, where oversight is carried out by a non-elected body, it should be required to report back to an elected representative regularly. It is worth noting that this reporting function may also play a useful role in assessing the agency's performance and management of public resources, in order to improve efficacy and efficiency.

While ultimate accountability to elected representatives is imperative, a strong system will also include one or more specialised administrative oversight bodies. If oversight is the purview of multiple organs, responsibility should be divided

along thematic lines rather than having each agency monitored by a different oversight structure. Oftentimes, the sum total of a surveillance system can be far more invasive when considered as a whole as opposed to being broken down into component parts. Ideally, compartmentalised oversight will be complemented by at least one agency with overall responsibility.

The ability to access relevant information is critical to effective oversight. For example, Section 7(8)(a) of South Africa's Intelligence Services Oversight Act grants the Inspector-General "access to any intelligence, information or premises under the control of any Service if such access is required by the Inspector-General for the performance of his or her functions, and he or she shall be entitled to demand from the Head of the Service in question and its employees such intelligence, information, reports and explanations as the Inspector-General may deem necessary for the performance of his or her functions".[89]

The independence of oversight bodies, both from intelligence agencies and from the executive, is crucial. Different States handle this task through a variety of mechanisms which can include courts, parliamentary oversight bodies, specialised administrative oversight bodies and civil society groups. In his 2009 report, the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism pointed to the Norwegian model of oversight as being particularly strong:

> *[I]t has an explicit human rights purpose, namely "to ascertain and prevent any exercise of injustice against any person" and to "ensure that activities are kept within the framework of statute law, administrative or military directives and non-statutory law". Furthermore, the parliamentary oversight committee is composed of seven members, who are appointed by Parliament but who don't necessarily have political affiliations. In this way the committee cannot be abused for party political games, a high level of expertise is guaranteed and the credibility of the expert-members is assured. The members are supported by a secretariat of three lawyers and one secretary who all have security clearance. The members have*

> *the power to compel the production of evidence to the committee concerning all matters experienced in the course of their duties. In pursuing its duties, the committee has access to the archives and registers, premises, and installations of all branches of the executive and the intelligence agency. [references omitted]*[90]

Since surveillance is always an interference with privacy, a measure of judicial oversight is also necessary. Judicial oversight should always be available to challenge alleged breaches of the rules after they have happened.

Independent prior approval of surveillance activities is also an important safeguard against abuse and is required as a default, albeit with exceptions, in many countries. The International Principles, for example, call for a competent judicial authority to approve any surveillance targets.

STANDARDS FOR LEGITIMATE SURVEILLANCE: ONLY NECESSARY INTRUSIONS

The necessity standard lies at the core of discussions over whether surveillance practices are appropriate. "Necessity" is generally understood as meaning, among other things, that an activity is the only means of securing a legitimate objective or, where there are multiple means, that it is the least intrusive one.

This standard is explicitly built into Article 33(2) of the *Act on the Security Intelligence System of the Republic of Croatia*:

> *The measures of secret information collection, which temporarily restrict certain constitutional human rights and basic freedoms, may be applied if the information can not be obtained in any other way or the collection thereof is linked with disproportionate difficulties. In cases where choice between several different measures of secret information collection is possible, the one less invasive to constitutionally protected human rights and basic freedoms shall be applied.*[91]

Proportionality, another component of necessity, involves weighing the harm done to rights through surveillance practices, which can often be subtle and indirect, against the benefits of the practice in terms of bolstering security or public order. The **chilling effect** of surveillance on expression or on people's willingness to use a particular platform is real and should be taken seriously. Although the chilling effect can be difficult to measure, there is evidence for the proposition that degrading **anonymity** harms online speech. For example, when Tech Crunch, a popular web forum for the discussion of technology products, changed its format to one which required users to attach their real name to any comments left, they found that the site, which had been known for hosting blistering criticism of sub-standard products, lost its scathingly honest character. Tech Crunch eventually reversed the move, with a plea for the commenters to come back.[92] Early research results suggest that, in the aftermath of the Snowden disclosures, searches on Google using privacy sensitive terms fell in the USA, UK and Canada.[93] It is worth noting that in other countries studied, notably Germany, South Korea and Saudi Arabia, this trend did not hold.

There is little question that bulk surveillance programmes along the lines of those revealed by the Snowden leaks raise serious concerns in terms of respect for privacy and freedom of expression. The revelations about the **Five Eyes** programmes have done more to undermine confidence in the security of the internet as a forum for expression than any other single event.

At the same time, serious questions have been raised over the benefits of blanket surveillance as well as the costs, in terms of diverting security agencies' time and attention. The failures of intelligence agencies to intercept the Boston Marathon bombers in 2013 and the attempted Christmas Day bombing by Umar Farouk Abdulmutallab are viewed by some as indicative of a misplaced focus on bulk surveillance to the detriment of traditional law enforcement methods. In both of those cases security agencies had received specific warnings about the attacks.[94] Hindsight is always twenty-twenty, and it is not completely fair to judge

the NSA's prioritisation decisions by its failure to follow up on two specific cases. At the same time, there have been very few concrete success stories from bulk data collection programmes.[95]

It is worth noting that China suffers from regular terrorist incidents, most recently on 1 March 2014 when 29 people were killed and a further 143 injured in an attack on a train station in Kunming, Yunnan.[96] In 2013 there were fatal attacks in Lukqun,[97] Taiyuan[98] and in Tiananmen Square in Beijing.[99] Of course, the fact that terror attacks continue to take place does not prove that China's web surveillance has been ineffective, since it is impossible to know whether other potential attacks were stopped. However, these attacks demonstrate that, even with an incredibly invasive surveillance system, serious security risks remain.

There have been very few concrete success stories from bulk data collection programmes.

Although less intrusive than the **Five Eyes** programmes, bulk **data retention** schemes also raise serious proportionality concerns due to their untargeted nature, as was noted by the ECJ in their ruling invalidating the Data Retention Directive. Despite the fact that the bulk of the information remains in private hands, these programmes nonetheless represent a loss of control over communications. There is also a risk that these databases could be **hacked**. In July 2012, when the Australian government announced that it was considering proposals to require Australian **ISPs** to retain data from their users, the Anonymous hacker network responded by promptly breaking into the database of a major ISP.[100]

The necessity standard suggests that the untargeted approach taken in many existing surveillance schemes may be illegitimate and that, instead, States are required to adopt a more directed approach based on a specific risk of harm. This would include a requirement that a serious crime had been committed or a degree of probability that one is likely to be committed, along with some nexus between the surveillance and the gathering of evidence regarding that crime.

Encryption

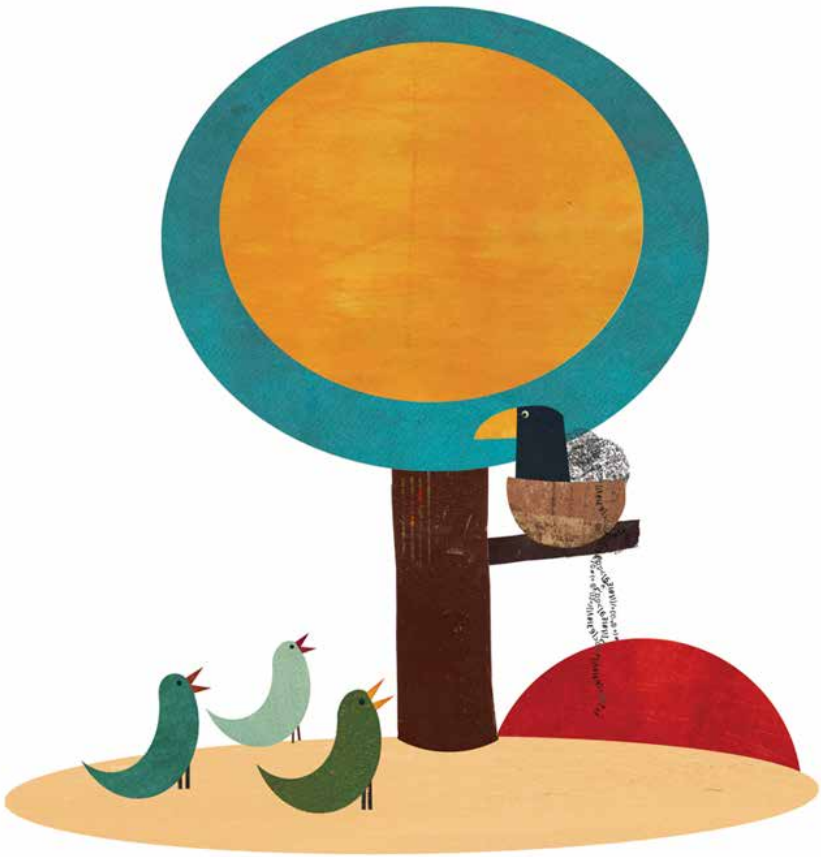
Attempts to undermine **encryption** techniques are very difficult to justify in terms of the proportionality test. The interest of this to security agencies is obvious; strong encryption systems are an effective tool for cyber-criminals or terrorists to avoid detection and capture. However, building weaknesses into the security systems of commonly used devices or deliberately inserting weak **algorithms** into encryption **software** poses serious risks to the integrity of these devices and the internet as a whole. While these approaches may be designed to allow access by security agencies, it is only a matter of time before they will be discovered by **hackers**. In a presentation on 30 December 2013, Jacob Appelbaum, a security researcher with access to the files leaked by Edward Snowden, congratulated two security researchers at the conference for having independently found a **backdoor** that the NSA had ordered to be built into certain computer systems.[101] Appelbaum noted that, for every security researcher whose work focused on finding and correcting vulnerabilities, there are hundreds of full time hackers working to find security holes, often for nefarious purposes. In other words, these programmes make everyone vulnerable, increasing the threat of cybercrime and eroding confidence in the security of the internet and digital technologies more broadly.

For every security researcher working to find and correct vulnerabilities, there are hundreds of hackers.

The scope for harm was clearly demonstrated by the discovery, in April 2014, of weaknesses in the **OpenSSL protocol**, dubbed the Heartbleed bug, which led to major disruptions of internet processes around the world. For example, according to the Canada Revenue Agency (CRA), at least 900 Canadians had their personal information stolen as they attempted to file their taxes online.[102] The CRA was forced to shut down its filing system temporarily during peak tax season as a result of the bug. There have been allegations that the NSA had known about the Heartbleed bug for years, and had exploited it to harvest passwords and other private information.[103] Though these allegations have been strenuously denied by the US government, it is worth noting that current policy, revised in January 2014, maintains that flaws which the NSA discovers in **software** can be kept secret if there is "a clear national security or law enforcement" use.[104] In other words, regardless of whether the NSA had advance knowledge of this particular bug, it is precisely the type of flaw which their policy suggests that they would keep secret, to exploit for their own purposes.

CHAPTER 3:

EMERGING DEBATES AND ACTIVISM



Emerging Debates And Activism

Concerns about the extent of online surveillance and its impact on privacy and freedom of expression did not begin with Edward Snowden. However, there is no question that the Snowden disclosures have reshaped the conversation around surveillance and drawn an enormous amount of attention to the issue. Along with State actors and the private sector, civil society has an important role to play in these debates as they unfold. This Chapter examines some of the more important current debates around surveillance in more detail, as well as the scope for civil society involvement in impacting change.

A GLOBAL UNDERSTANDING OF DIGITAL RIGHTS

Although it has long been recognised that basic human rights, such as freedom of expression and privacy, apply to online communications, the transition has been conceptually tricky. The online world has its own unique culture, which does not always align with the human rights standards developed in an offline context.

The Snowden leaks have raised serious questions about respect for human rights on the internet in the developed, democratic world, where a significant number of internet users are based. Citizens of the United States and Europe had become inured to stories of censorship in China or Iran and took it for granted that threats to core human rights were a problem that happens "over there". The revelation that the **Five Eyes** governments are behind the world's most pervasive global surveillance apparatus has forced a reconsideration of the accepted narrative that issues of internet

freedom are black and white, and pit open and progressive States against closed and repressive ones.

At the very least, this requires a shift in advocacy strategies. Where previously activist organisations in the developed world would focus on providing support and capacity building to their developing world counter-parts on the "front lines", the internet has globalised problematic domestic practices. China's **Great Firewall** not only hurts Chinese internet users, it hurts everyone on the internet by limiting their ability to interact with people in China. The NSA's surveillance practices are ostensibly only targeted at non-US citizens, but by chilling speech on the internet they damage the medium for people in the US as much as anyone else.

"Citizens of the United States and Europe took it for granted that threats to core human rights were a problem that happens "over there".

The cooperation agreements between intelligence agencies spelled out in Chapter 1 amply illustrate the problem with applying pre-digital understandings of jurisdiction to an online context. It is a simple enough matter for the GCHQ to outsource surveillance of Britons to, for example, Canada's CSE, and vice versa. But these problems also illustrate a more fundamental way in which historical understandings of human rights are themselves outdated in a digital world. While human rights have traditionally been understood to apply to how States treat their citizens and others falling within their jurisdiction, this fails to account for the drastic global impact that a single State's internet policies can have. In an online world, States must increasingly take responsibility for the extra-territorial effect of their actions.

Getting involved

On 12 March 2014, the 25th anniversary of when Sir Tim Berners-Lee first proposed the creation of the **world wide web**, the British scientist announced that the World Wide Web Consortium would be launching a campaign for an Internet Bill of Rights.105 Although it was announced with great fanfare, this is not a new idea. The Internet Rights and Principles Coalition has already developed a Charter of Human Rights and Principles for the Internet.106 And the Internet Rights Charter, by the Association for Progressive Communications, was released as far back as 2006.[107]

It will, of course, be a major challenge to try to get a binding document on internet rights adopted at the international level. Understandings of core concepts like privacy vary enormously from country to country. In Germany, for example, the legacy of the Nazis and, more recently, the Stasi, the repressive East German secret police force, is often credited for strong German antipathy towards invasive surveillance systems. Once one moves beyond the issue of privacy into more specific surveillance questions, which are just one of the major issues a new agreement would need to address, issues of due process, judicial fairness and the importance of or right to **anonymity** would also need to be resolved, a difficult task.

Perhaps in anticipation of this problem, Sir Tim Berners-Lee is proposing to promote digital rights at the national, rather than at the international, level. Again, this is not new. Several digital rights bills have been proposed, most notably Brazil's Internet Bill of Rights. However, there are drawbacks to this approach. For example, it is impractical to expect websites to align their practices with dozens of competing standards for privacy, tracking, transparency and so on. National approaches will also be ineffective in limiting the ability of external surveillance agencies to ply their trade.

However, there is still value in pursuing digital rights at a national level. Brazil's "Internet Bill of Rights" is a victory for internet users everywhere, which will hopefully set an example for more States to codify human rights on the internet. The We Promise Campaign, in which European civil society groups have joined forces to insert digital rights concerns into the 2014 EU Parliament elections, is another good example of advocacy aimed at a single legislative body.[108]

However, ultimately national and even continental understandings must be viewed as a means to the goal of a unified global understanding of digital rights as cross-cultural and international concepts. Establishing broadly embraced and respected principles represents a major challenge for civil society around the world. Networking, collaborating and sharing experiences, values and challenges are essential foundational activities which civil society needs to undertake to lay the groundwork for building a common global understanding of digital rights.

Ultimately national and even continental understandings must be viewed as a means to the goal of a unified global understanding of digital rights as cross-cultural and international concepts.

STRUCTURAL AND TECHNICAL IMPLICATIONS FOR THE INTERNET

The **Five Eyes** surveillance programme has led to a major loss in confidence in the United States as a force for internet freedoms. While it is too early to judge the impact this will have on the internet as a whole, major structural changes are being considered. In September 2013, following revelations of extensive surveillance against Brazilian governmental and economic interests, Brazilian President Dilma Rousseff announced plans for an undersea **fibre-optic cable** to connect South America with Europe, bypassing the need to route traffic through the United States.[109] Although this would make data collection more difficult than the current model, under which nearly all communications from Latin America run through the "Network Access Point of the Americas" in Miami, some analysts believe the NSA will find a workaround, pointing to reports that the agency has a nuclear submarine capable of tapping undersea fibre-optic lines.[110]

Another scheme, known as "Schengen routing", has been championed by Germany, another country whose leadership was extensively targeted by the NSA. The idea behind this proposal would be to keep as much traffic on the European mainland (excluding the United Kingdom) as possible.[111] However, this system also faces doubts as to its efficacy, given that Schengen countries such as Holland have been known to collaborate closely with NSA programmes.

Forcing traffic to take a particular geographic path would decrease the efficiency of the system.

While they may seem like an attractive solution to wary Brazilians or Germans, schemes which aim to alter the flow of traffic across the internet have profound implications. Under the current model, internet **routers** send information via the cheapest and fastest route, without regard for national boundaries. There is no harm to adding new connections, such as Brazil's proposed direct link to Europe, but imposing artificial restrictions on how and where internet traffic can flow would decrease the efficiency of the system, raising prices and reducing connection speeds.

Moves to reshape the internet's structure along national or regional lines also give rise to the threat that the Web will become **balkanised**. A great value of the internet is its borderless nature and its ability to connect users from different cultures. One high profile example of this was the "Israel Loves Iran" campaign where, during a time of heightened tension between the two countries, an Israeli artist encouraged his countrymen to post positive messages about Iran on a Facebook page. The campaign went viral and was soon complemented by a parallel "Iran Loves Israel" campaign.[112] Although it would be naïve to think that the world's major geopolitical conflicts can be solved through Facebook campaigns, there is nonetheless tremendous value in this kind of dialogue and in the internet's role in bringing together people from States that are experiencing hostilities towards one another. Routing changes along the lines proposed by Brazil and Germany would not themselves have precluded these campaigns from taking place, but they do represent a move towards imposing territorial borders on what has hitherto been a largely borderless medium.

At the moment, countries like China, which impose significant border controls over internet traffic, are outliers. With the notable exception of South Korea, which censors pro-North Korean content, in democratic States the internet remains largely free and open.[113] If traffic restrictions became commonplace, this would threaten to muddy the waters between States which facilitate free access to the internet and those which do not.

Getting involved

Given that proposals to restrict the way that information flows across the internet are ultimately driven by a desire to protect human rights, it is not surprising that civil society has played a key role in this discourse. At the State level, Brazil has been at the vanguard of a recent push for enhancing digital rights, notably through its passage in April 2014 of an "Internet Bill of Rights".[114] However, in addition to advocating in favour of the Bill's passage, civil society played a key role, alongside the private sector, in convincing the government that proposed requirements for cloud service providers to store data on Brazilians within Brazil would be ineffective and counterproductive towards the goal of safeguarding user privacy.[115]

In other words, civil society has a key role in ensuring that State-level responses to the **Five Eyes** surveillance revelations do not threaten broader freedom of expression interests. Private sector interests, particularly in the telecommunications industry, can be important allies in this conversation due to their shared interest in preserving the efficiency of the current model of routing.[116]

INTERNET GOVERNANCE

For years, there has been significant debate around whether the internet's governance structure, which is currently dispersed across a range of actors and institutions, should be reformed. Many proponents for reform argue that power in the current system is disproportionately concentrated in US-based organisations, while others point to the system's ineffectiveness in the absence of a single forum where stakeholders can develop binding international rules on all internet issues. Two main, overlapping, groups lead the calls for change. On the one hand a number of authoritarian governments, reacting to growing

evidence that the internet is a remarkably effective tool for citizen mobilisation, are calling for new mechanisms for greater governmental control. On the other hand, there is a range of governments, as well as non-governmental stakeholders, who are dissatisfied with a regime where it is not clear where and how international internet policy is made, where businesses can often act without restrictions, and where more powerful countries set rules that are forced on everyone else. The perceived lack of fora for addressing a whole array of issues, ranging from cybersecurity to internet access and surveillance, which has become a driving concern since the Snowden revelations, mean that some governments wish to revert to a traditional multilateral governance framework.

Against these calls for change, the United States and some of its allies have been vigorously defending the status quo. They argue that the current regime, lacking centralised governmental oversight, has contributed to the rapid spread of the internet across the world and the strong internet culture of freedom of expression and innovation. This is to some extent true, but the US has also benefitted disproportionately from the rapid spread of the internet. Major internet companies are disproportionately US-based, which means that the US government is able to exercise additional control over them, as became apparent with Edward Snowden's revelations of arbitrary mass-surveillance.

In light of these revelations, however, the status quo position has become untenable, and change seems inevitable. The internet governance organisations have become increasingly assertive about the need to distance themselves from the United States government. On 7 October 2013, the leaders of the organisations responsible for coordinating the internet's technical infrastructure issued the Montevideo Statement on the Future of Internet Cooperation, which stressed the need for "accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing." In April 2014

the Brazilian government, as a direct response to the Snowden revelations, hosted "Net Mundial", a multi-stakeholder meeting on the future of internet governance with the aim of developing principles for internet governance, and a roadmap for evolving the internet governance regime.

Although there was some disappointment among civil society that Net Mundial's final outcome document failed to adequately reflect key concerns (including over online surveillance), the following years will see a range of international meetings which have the potential to fundamentally alter the way that the internet is governed at the global level. This includes the forums where decisions are passed, and the shape of those forums including whether or not civil society is adequately represented.

Getting involved

What change will look like is far from clear, and reaching consensus between deeply polarised views seems unlikely in the short term. This presents an enormous opportunity for civil society to step into the gap and make positive recommendations on the way forward. It's an opportunity to hard-bake human rights and good governance standards – with a clear and meaningful role for civil society – into all internet governance mechanisms and processes. As a global medium, it is also vital that the internet's governance structures represent the interests of the developing, as well as the developed, world. On the other hand, many actors are pushing for less transparent and inclusive governance structures so civil society must stay vigilant. Civil society organisations and networks have a unique ability to present a united and consistent international front in support of a free and open internet, and against government and private sector interests working counter to that goal.

SHIFTING BUSINESS CLIMATES

Another major debate that has grown out of the Snowden leaks has been over the trustworthiness of US-based technology firms. In the months since the Snowden leaks, US companies have faced significant blowback, particularly in Europe and South America. Market analysts estimate that US companies could lose USD35-180 billion by 2016 as a result of the damage to their reputations.[117] Perhaps unsurprisingly, the threat to their bottom-lines has led US companies to become prominent supporters of efforts to curb the data surveillance programmes. Several of the biggest players, including Microsoft, Google, Yahoo, Facebook, Apple and AOL, have lobbied in favour of the USA FREEDOM Act, which would significantly curb the NSA's powers.[118] RSA Securities, the firm which allegedly collaborated to weaken **encryption** standards, has called for the NSA to be split into two, dividing their security branch from their intelligence gathering arm.[119] It is too early to tell whether there will be a permanent trend away from US-based products and services, but the fact that major business interests are lining up in favour of curbing the intelligence gathering powers of the NSA is a significant development given the importance of money in US politics.

Several of the world's biggest tech companies have become prominent campaigners against NSA surveillance.

The backlash against US technology is somewhat ironic given the fact that, for years, Western companies were seen as a more trustworthy alternative, given fears of surveillance from Chinese firms. Huawei, a major telecommunications provider which has faced frequent accusations of complicity in Chinese espionage, announced in December 2013 that it would no longer bid for large service contracts in the United States, stating concerns related to NSA surveillance.[120]

However, it is important to note that concerns about Chinese technology are legitimate, and that Huawei's move was likely more about playing up the public relations value of this odd role-reversal than any real concern about complicity in surveillance.

The main beneficiaries of moves in Europe and South America away from US technology have been smaller, domestic alternatives in those regions. An apparently common joke among German tech companies is that Edward Snowden is the best marketing employee they have.

For some, however, the dramatic loss of confidence in US-products is an argument for moving to more **open source** models of **software** development. There is an argument that many eyes make safe **code**, and that the open nature of programs such as Linux or Firefox improves their security. There is a counter-argument that the involvement of hobbyists in developing some open-source programs and an emphasis on functionality rather than security makes them less safe on the whole. However, there is no question that open-source products are far more difficult, although not impossible, to **backdoor**.[121]

Getting involved

Given that **open source** projects rely on community participation, this is a clear opportunity for civil society to contribute to making the internet a more secure place. Although volunteers with coding skills are most obviously needed, there are a range of participation options for those without programming skills. For example, Mozilla relies on volunteers to translate its programs into new languages, test out **software** under development to find bugs and assist with marketing, education and other creative promotional activities.[122] Similarly, anyone with an internet connection can also assist the **Tor** project by donating bandwidth.[123] Civil society organisations can also play a key role in sharing these technologies with activists or journalists who face a more pressing need for **encryption** or anonymisation software.

TOWARDS AN ENCRYPTED WEB

At a consumer level, there is evidence that the Snowden leaks have led to an increase in interest in **anonymity** and security. Between June 2013, when the Snowden leaks began, and January 2014, the use of anonymous search engines Ixquick and Startpage almost doubled,[124] while usage of the **Tor** anonymisation tool tripled over the same period.[125]

There has also been increased interest in **encryption**.[126] Microsoft and Google have both announced significant expansions in their default use of encryption[127] and Brazil's post office is reported to be developing an encrypted public email program.[128]

Other reactions have been more drastic. In July 2013, it was reported that Russia's Federal Guard Service, which oversees government communications, was purchasing $15,000 worth of electric typewriters for use in preparing secret documents.[129] An article in the Economist advised surveillance-wary readers to remove the batteries on their mobile phone and store them in the refrigerator when not in use.[130]

Paranoia is hardly conducive
to a free and open internet.

The internet belongs to everyone and everyone should have a say in its future direction. Activists and researchers have a key role to play in unifying understandings of digital rights and in challenging problematic practices. We hope that this Guide will not only help you to understand the current debate over surveillance, but will also inspire you to mobilise and engage, so that users everywhere will assert their right to a free and open internet.

Getting involved

Although this level of paranoia is hardly conducive to a free and open internet, stronger public awareness of online security is a positive development. In addition to the steps suggested in the previous section, such as supporting projects that increase security and sharing information, civil society should lead by example and take steps to **encrypt** their own communications as far as possible. A good first step is to create an **HTTPS** version of the organisation's website.

Glossary

algorithm A process or set of rules that a computer follows in order to complete a calculation.

anonymity The ability to act online without those actions being tied to your legal identity.

backdoor A method for bypassing the security or authentication settings in a computer system.

balkanised A non-technical term which is often used to describe attempts to fragment the internet into national units, for example Iran's attempts to build a National Information Network

chilling effect A state of affairs where expression is inhibited, particularly as a result of the imposition of sanctions on certain types of expression. Note that this effect tends to be amplified beyond the prohibited behaviours themselves as users seek to steer well clear of the line.

code A set of instructions for a computer to facilitate a particular function.

data protection Legal protection for an internet user's personal information. At a very general level, these regimes place conditions on the collection, use and storage of personal data, give certain rights to the individuals to whom the data relates, and provide for a system of oversight to ensure respect for the rules and to address breaches.

data retention The preservation of an archive of data. Data retention mandates, usually imposed upon communications service providers, require storage of particular types of information about how their systems have been used and by whom for a particular period of time.

distributed denial of service attacks The act of preventing or slowing access to an internet resource by flooding it with bogus requests. Attacks are "distributed" in the sense that all these requests purport to come from different locations, making them hard to block.

economic espionage Spying which is carried out for commercial reasons or to obtain a commercial advantage.

encryption A process of encoding messages so that they can only be understood by parties holding decryption tools.

exploit A piece of **software** that "exploits" a vulnerability in another piece of software, for example allowing it to be controlled remotely or used in a **distributed denial of service attack**.

fibre-optic cable A cable containing a bundle of glass or plastic fibres which carry pulses of light used to convey information. They are a primary means for transporting bulk information over the internet.

filters Software that inspects data packets travelling across the internet infrastructure for key information and blocks or re-routes traffic containing that content.

five eyes A cooperative surveillance agreement that exists between spy agencies in Australia, Canada, New Zealand, the UK and the USA. The Five Eyes agencies also cooperate with other nations through more limited agreements.

Great Firewall of China Colloquial term for the Golden Shield Project, China's pervasive State apparatus designed to censor, monitor and otherwise control domestic use of the internet.

ground station A terrestrial terminal station designed to receive communications signals from an extra-terrestrial source, such as a **satellite**.

hacking Bypassing, without authorisation, the security protections of an information system or network.

HTTPS Hypertext Transfer Protocol Secure. HTTPS is an update on the underlying protocol used to transmit messages by the world wide web which makes that communication more secure.

internet exchange point A physical structure where **ISPs** interconnect their equipment to facilitate the movement of information between their networks.

internet service providers (ISP) Organisations that provide access to the internet and (commonly) operate parts of the network that make it up.

iOS A mobile operating system developed by Apple.

IP Internet Protocol. The code which labels packets of data sent across the internet, identifying both the sending and the receiving computers.

Kim Dotcom An internet entrepreneur and hacker who founded Megaupload, a popular file-hosting website. The website was shut down by the United States Department of Justice in 2012 and the owners were charged with criminal copyright infringement. Kim Dotcom is currently in New Zealand fighting extradition to the US.

malicious software Also known as malware, code designed to compromise someone's computer.

metadata Literally "data about data", this term is often applied to information about web traffic.

network management The process of managing a computer network so as to maximise its security, performance and reliability.

online behavioural tracking A technique for collecting and interpreting users' browsing data to build a profile, especially for use in advertising.

open source software the **source code** of which is made freely available, allowing users to modify it themselves.

OpenSSL protocol An open-source code that creates a secure connection between a client and a server for transmitting sensitive data, such as credit card numbers.

PRISM A mass electronic surveillance system launched by the United States' National Security Agency in 2007. It mines data stored by a range of internet intermediaries.

quantum supercomputer A computer that makes use of quantum-mechanics to process data much quicker speeds than normal computers.

right to information A right found in many jurisdictions which empowers citizens to access information under the control of public authorities and, in some instances, private authorities..

routers A piece of networking hardware that forwards data packets around a network.

satellite A type of network connection using hardware that orbits the Earth.

servers A computer that hosts content on the internet, such as emails or websites.

software The programs used by a computer, including those programs designed to operate and control the computer hardware (such as the operating system) and applications software (such as office suites).

source code is the version of software as it is originally written in plain text readable by humans. A programmer will then translate it into machine-language format.

Tor A program which uses layered encryption, as well as a virtual information circuit, to allow users to browse the web anonymously. "TOR" originally stood for "The Onion Router".

upstream collection The term used by the United States' National Security Agency for intercepting internet traffic directly from major internet cables and switches, rather than through intermediary companies.

viruses Malicious computer code capable of copying itself. Viruses destroy data or have some other negative effect on their host computers.

world wide web A system of interlinked files and documents on the internet, navigated using a web browser (e.g. Mozilla Firefox, Internet Explorer).

Further Reading

Association for Progressive Communications A global network and organisation working on internet access, rights and governance issues: http://www.apc.org/

Canadian Privacy Law Blog Privacy blog with an emphasis on digital issues operated by David Fraser, a Canadian lawyer: http://blog.privacylawyer.ca

Centre for Democracy and Technology A US-based NGO that focuses on digital rights: http://www.cdt.org

Centre for Law and Democracy A Canada-based NGO which is active on digital rights issues: http://www.law-democracy.org

Cryptocat A free encrypted instant-messaging program: https://crypto.cat

Deep Packet Inspection Explained A relatively straightforward explanation of a complicated surveillance tool: http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works

Electronic Frontiers Foundation A US-based NGO that focuses on digital rights: https://www.eff.org

Enemies of the Internet A roundup of digital threats by Reporters Without Borders: http://surveillance.rsf.org/en/

European Digital Rights Initiative A European NGO that focuses on digital rights: http://edri.org

Front Line Defenders The International Foundation for the Protection of Human Rights Defenders and creators of a manual on Digital Security and Privacy for Human Rights Defenders: http://www.frontlinedefenders.org/

F-Secure Blog A digital security blog operated by Mikko Hyppönen, a Finnish security expert: http://www.f-secure.com/weblog/

Global Partners Digital A UK-based organisation working on international internet rights and governance issues: http://www.gp-digital.org/

Internews An international organisation working to empower local media. They have developed the "Media Workers' Toolkit for Safer Online and Mobile Practices": https://www.internews.org/

Mozilla A technology collective best known for developing Firefox, an open-source web browser: http://www.mozilla.org

Jitsi An open source encrypted videoconferencing and instant messaging application: https://jitsi.org

Prism Break A website which provides a list of systems, services and platforms for evading surveillance: http://prism-break.org/en/

The Intercept An online publication founded by Glenn Greenwald, Laura Poitras and Jeremy Scahill which serves as the primary platform for reporting on the Snowden leaks: https://firstlook.org/theintercept/

Tactical Technology Collective An international organisation that creates many digital guides and trainings, including on digital security skills: https://www.tacticaltech.org/

The Tor Project An anonymisation tool which, although partially funded by the US government, is apparently resilient to tracking efforts: https://www.torproject.org[131]

Endnotes

1 Tom Bowman and Scott Shane, "America's Fortress of Spies", *Baltimore Sun*, 3 December 1995. Available at: articles.baltimoresun.com/1995-12-03/news/1995337001_1_intelligence-agency-nsa-intelligence-national-security-agency.

2 R. James Woolsey, "Why We Spy on Our Allies", *Wall Street Journal*, 17 March 2000. Available at: online.wsj.com/news/articles/SB95326824311657269.

3 Although the past tense is used here, it is impossible to confirm whether the programme was ever terminated. Echelon may still be operating or it may have been subsumed into the broader data collection schemes that have been established since the spread of the internet.

4 Available at: www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN.

5 "No spying on friends: NSA bugs Merkel aides instead of chancellor", *RT News*, 24 February 2014. Available at: rt.com/news/nsa-germany-spying-switch-384.

6 James Gordon Meek, Luis Martinez and Alexander Mallin, "Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security", *ABC News*, 29 January 2014. Available at: abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388.

7 Craig Timberg, "The NSA slide you haven't seen", *Washington Post*, 10 July 2013. Available at: www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.

8 Full testimony available at: www.eff.org/node/55051.

9 Siobhan Gorman and Jennifer Valentino-Devries, "New Details Show Broader NSA Surveillance Reach", *Wall Street Journal*, 20 August 2013. Available at: online.wsj.com/news/articles/SB95326824311657269.

10 Dana Priest and William M. Arkin, "A hidden world, growing beyond control", *Washington Post*, 19 July 2010. Available at: projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print/.

11 James Bamford, The NSA Is Building the Country's Biggest Spy Center (Watch What You Say), *Wired*, 15 March 2012. Available at: www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/.

12 *Ibid.*

13 "NSA slides explain the PRISM data-collection program", *Washington Post*, 6 June 2013. Available at: www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

14 Ewen MacAskill, "Yahoo files lawsuit against NSA over user data requests", *Guardian*, 9 September 2013. Available at: www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests.

15 Erik Kain, "The NSA Reportedly Has Total Access To The Apple iPhone", *Forbes*, 30 December 2013. Available at: www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone/.

16 Matthew Panzarino, "Apple Says It Has Never Worked With NSA To Create iPhone Backdoors, Is Unaware Of Alleged DROPOUTJEEP Snooping Program", *Tech Crunch*, 31 December 2013. Available at: techcrunch.com/2013/12/31/apple-says-it-has-never-worked-with-nsa-to-create-iphone-backdoors-is-unaware-of-alleged-dropoutjeep-snooping-program/.

17 Frederic Lardinois, "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program", Tech Crunch, 6 June 2013. Available at: techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/.

18 Spencer Ackerman, "US tech giants knew of NSA data collection, agency's top lawyer insists", *Guardian*, 19 March 2014. Available at: www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de.

19 Chris Duckett, "Verizon exec slams Google, Microsoft, Yahoo for NSA lawsuit grandstanding", *ZD Net*, 17 September 2013. Available at: www.zdnet.com/verizon-exec-slams-google-microsoft-yahoo-for-nsa-lawsuit-grandstanding-7000020769.

20 Joseph Menn, "Exclusive: Secret contract tied NSA and security industry pioneer", *Reuters*, 20 December 2013. Available at www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

21 Steven Rich and Barton Gellman, "NSA seeks to build quantum computer that could crack most types of encryption", *Washington Post*, 2 January 2014. Available at: www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.

22 James Ball, "NSA and GCHQ target Tor network that protects anonymity of web users", *Guardian*, 4 October 2013. Available at: www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

23 Full testimony is available at: site.d66.nl/intveld/document/testimony_snowden/f=/vjhvekoen1ww.pdf.

24 An analysis of the problems with this law can be accessed at: www.law-democracy.org/live/wp-content/uploads/2013/07/Russia.final_.pdf.

25 Edward Snowden, "Vladimir Putin must be called to account on surveillance just like Obama", *Guardian*, 18 April 2014. Available at: www.theguardian.com/commentisfree/2014/apr/18/vladimir-putin-surveillance-us-leaders-snowden.

26 Runa Sandvik, "Ethiopia Introduces Deep Packet Inspection", *The Tor Blog*, 31 May 2012. Available at: blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection.

27 "Phobos", "Iran partially blocks encrypted network traffic", *The Tor Blog*, 10 February 2012. Available at: blog.torproject.org/blog/iran-partially-blocks-encrypted-network-traffic.

28 "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", *The Tor Blog*, 16 February 2012. Available at blog.torproject.org/blog/kazakhstan-upgrades-censorship-deep-packet-inspection.

29 See: surveillance.rsf.org/en/china.

30 *Ibid.*

31 Phelim Kine, "China's Internet Crackdown", *Forbes*, 27 May 2010. Available at: www.forbes.com/2010/05/27/china-internet-web-censor-surveillance-technology-security-google-yahoo-green-dam.html.

32 Ivan Sigal, "Libya: Foreign Hackers and Surveillance", *Global Voices Advocacy*, 26 October 2011. Available at: advocacy.globalvoicesonline.org/2011/10/27/libya-foreign-hackers-and-surveillance/.

33 Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens", *Bloomberg*, 22 August 2011. Available at: www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

34 Andy Greenberg, "Nokia Siemens Denies Lingering Ties To Iran Surveillance", *Forbes*, 15 October 2010. Available at: www.forbes.com/sites/andygreenberg/2010/10/15/nokia-siemens-denies-lingering-ties-to-iran-surveillance/.

35 See: citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf.

36 See: surveillance.rsf.org/en/blue-coat-2/.

37 Available at: bluecoat.com/company/ethics-policy-partners.

38 Report available at: citizenlab.org/2013/04/for-their-eyes-only-2/.

39 For example, many telecommunications providers collect data for billing purposes.

40 Alexandra Kulikova, "Data Collection and Retention in Russia: Going Beyond the Privacy and Security Debate", *Global Partners Digital*, 17 January 2014. Available at: www.gp-digital.org/gpd-update/data-collection-and-retention-in-russia/. "China: MIIT launches plans to extend data retention for IISPs", *Privacy This Week*, 19 July 2012. Available at: www.dataguidance.com/dataguidance_privacy_this_week.asp?id=1818.

41 Case C-293/12. Available at: curia.europa.eu/juris/documents.jsf?num=C-293/12.

42 Similar problems were noted in an analysis carried out in 2013 by Centre for Law and Democracy, available at: www.law-democracy.org/live/european-union-data-retention-directive-not-justifiable/.

43 Available at: www.law-democracy.org/wp-content/uploads/2010/07/Thai.Computer.Jul07.official.pdf.

44 Centre for Law and Democracy's analysis of the Thailand Computer Crime Act, B.E.2550 is available at: www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

45 Law No. 10 of 2009. Available at: deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

46 See Centre for Law and Democracy's full analysis of the Cybercrime Prevention Act of 2012 at: www.law-democracy.org/live/wp-content/uploads/2012/11/Phil.Cybercrime.final_.pdf.

47 Phoebe Magdirila, "Philippines' Cybercrime Law now in effect, punishing online libel is constitutional", *Tech in Asia*, 18 February 2014. Available at: chinasia.com/philippines-cybercrime-law-effect-punishing-online-libel-constitutional/.

48 Edward Moyer, "NSA offers details on 'LOVEINT' (that's spying on lovers, exes)", *CNET*, 27 September 2013. Available at: news.cnet.com/8301-13578_3-57605051-38/nsa-offers-details-on-loveint-thats-spying-on-lovers-exes/.

49 Spencer Ackerman and James Ball, "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ", *Guardian*, 28 February 2014. Available at: www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

50 Jonathan Watts, "NSA accused of spying on Brazilian oil company Petrobras", *Guardian*, 9 September 2013. Available at: www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras. "Brazil accuses Canada of spying after NSA leaks", *Guardian*, 8 October 2013. Available at: www.theguardian.com/world/2013/oct/08/brazil-accuses-canada-spying-nsa-leaks.

51 Cyrus Farivar, "New Zealand appears to have used NSA spy network to target Kim Dotcom", *Ars Technica*, 23 August 2013. Available at: arstechnica.com/tech-policy/2013/08/new-zealand-appears-to-have-used-nsa-spy-network-to-target-kim-dotcom/.

52 Vernon Loeb, "NSA Admits to Spying on Princess Diana", *Washington Post*, 12 December 1998. Available at: www.washingtonpost.com/wp-srv/national/daily/dec98/diana12.htm.

53 Andrei Soldatov and Irina Borogan, "Journalists to be under digital surveillance at Sochi", Committee to *Protect Journalists Blog*, 28 January 2014. Available at: cpj.org/blog/2014/01/journalists-to-be-under-digital-surveillance-at-sochi.php.

54 See surveillance.rsf.org/en/bahrain/.

55 Stephan Faris, "The Hackers of Damascus", *Bloomberg Businessweek*, 15 November 2012. Available at: www.businessweek.com/articles/2012-11-15/the-hackers-of-damascus.

56 Luke Harding, "Edward Snowden: US government spied on human rights workers", *Guardian*, 8 April 2014. Available at: www.theguardian.com/world/2014/apr/08/edwards-snowden-us-government-spied-human-rights-workers.

57 Leonard Downie Jr., "The Obama Administration and the Press", *Committee to Protect Journalists*, 10 October 2013. Available at: cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.

58 UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988. Available at: www.refworld.org/docid/453883f922.html.

59 UN General Assembly Resolution 217A(III) of 10 December 1948.

60 UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.

61 Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.

62 *Big Brother Watch and others v. United Kingdom*, 4 September 2013, Application no. 58170/13 (European Court of Human Rights). Available at: hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713.

63 *Malone v. The United Kingdom*, 2 August 1984, Application no. 8691/79 (European Court of Human Rights). Available at: hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533.

64 2000, c. 23. Available at: www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf.

65 *Brannigan and McBride v. The United Kingdom*, Application no. 14553/89 (European Court of Human Rights), para. 43. Available at: hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57819.

66 Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 *European Journal of Information Systems* (2013), p. 300. Available at: www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.

67 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, UN Doc. A/HRC/23/40, para. 79.

68 Council of Europe, *Declaration on Freedom of Communication on the Internet*, Principle 7 (2003). Available at: www.coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf.

69 Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.

70 Resolution A/HRC/20/L.13. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.

71 Resolution A/C.3/68/L.45/Rev.1, Adopted 26 November 2013. Available at:

www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

72 Available at: www.cidh.oas.org/Terrorism/Eng/part.p.htm.

73 Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/10session/A.HRC.10.3.pdf.

74 Note 67, para. 3.

75 Adopted 21 June 2013. Available at: www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

76 Opening Remarks to the Expert Seminar: The right to privacy in the digital age, 24 February 2014. Available at: www.ohchr.org/AR/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=A.

77 20-20 Human Rights Vision Statement for Human Rights Day, 10 December 2013. Available at: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14074

78 Available at: en.necessaryandproportionate.org/text#_ednref2.

79 General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 25.

80 Act No. 113 of 1979 as amended. Available at: www.comlaw.gov.au/Details/C2012C00260.

81 Enacted 30 June 2006. Available at: www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf.

82 7 December 1999. Available at: www.planalto.gov.br/ccivil_03/Leis/L9883.htm [in Portuguese. Translated via Google].

83 See *Claude Reyes and Others v. Chile*, 19 September 2006, Series C, No. 151 (Inter-American Court of Human Rights) and *Társaság A Szabadságjogokért v. Hungary*, 14 April 2009, Application no. 37374/05 (European Court of Human Rights).

84 Available at: www.right2info.org/resources/publications/laws-1/laws_ghana_rti-law.

85 Available at: www.ip-rs.si/index.php?id=324.

86 Translated by the author. Law is available in Spanish at: www.cartercenter.org/resources/pdfs/peace/americas/nicaragua_2007_law.pdf.

87 Opening Remarks to the Expert Seminar: The right to privacy in the digital age, 24 February 2014. Available at: www.ohchr.org/AR/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=A.

88 Available at: english.nmhh.hu/dokumentum/150102/125_1995_torv_eng_lekt_20070515.pdf.

89 Act 40 of 1994. Available at: www.oigi.gov.za/Legislation/IntelServicesOversightAct40of1994.pdf.

90 Report available at: www2.ohchr.org/english/bodies/hrcouncil/docs/10session/A.HRC.10.3.pdf.

91 Enacted 30 June 2006. Available at: www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf.

92 Matt Burns and Elin Blesener, "Commenters, We Want You Back", 22 January 2013, *Tech Crunch*. Available at: techcrunch.com/2013/01/22/we-want-you-back/.

93 Alex Marthews and Catherine Tucker, "Government Surveillance and Internet Search Behavior", 24 March 2014. Available at: ssrn.com/abstract=2412564.

94 Karen DeYoung and Michael Leahy, "Uninvestigated terrorism warning about Detroit suspect called not unusual", Washington Post, 28 December 2009. Available at: www.washingtonpost.com/wp-dyn/content/article/2009/12/27/AR2009122700279.html. Scott Shane, Michael S. Schmidt and Eric Schmitt, "Russia's Warning on Bombings Suspect Sets Off a Debate", *New York Times*, 25 April 2013. Available at: www.nytimes.com/2013/04/26/us/russia-told-us-bomb-suspect-was-radical-islamist.html?_r=0.

95 Ellen Nakashima, "NSA cites case as success of phone data-collection program", *Washington Post*, 8 August 2013. Available at: www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html.

96 Patrick Brown, "Kunming knife attacks show China has a terrorism problem too", *CBC*, 3 March 2014. Available at: www.cbc.ca/news/world/kunming-knife-attacks-show-china-has-a-terrorism-problem-too-1.2558573.

97 Matt Schiavenza, "35 People Dead in Chinese Mass-Murder: What Happened?", *The Atlantic*, 3 July 2013. Available at: www.theatlantic.com/china/archive/2013/07/35-people-dead-in-chinese-mass-murder-what-happened/277463/.

98 "Blasts at China regional Communist Party office kill one", *BBC*, 6 November 2013. Available at: www.bbc.com/news/world-asia-china-24830724.

99 Benjamin Kang Lim and Ben Blanchard, "China suspects Tiananmen crash a suicide attack- sources", *Reuters*, 29 October 2013. Available at: www.reuters.com/article/2013/10/29/us-china-tiananmen-idUSBRE99S02R20131029.

100 Joel Falconer, "Anonymous hacks Australian ISP AAPT to demonstrate data retention problems", *The Next Web*, 26 July 2012. Available at: thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems/.

101 Full presentation available at: www.youtube.com/watch?v=vIL.AlhwUgIU.

102 Richard Blackwell and Tu Thanh Ha, "Tax agency leaves Heartbleed victims in the dark about stolen data", Globe and Mail, 14 April 2014. Available at: www.theglobeandmail.com/technology/sin-numbers-stolen-from-tax-agency-website-using-heartbleed-bug/article17956353/.

103 Michael Riley, "NSA Said to Exploit Heartbleed Bug for Intelligence for Years", *Bloomberg*, 12 April 2014. Available at: www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html.

104 Kim Zetter, "Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA", Kim Zetter, *Wired*, 15 April 2014. Available at: www.wired.com/2014/04/obama-zero-day/.

105 Costas Pitas, "World Wide Web creator Tim Berners-Lee calls for a digital bill of rights to ensure internet freedom", Sydney Morning Herald, 13 March 2014. Available at: www.smh.com.au/digital-life/digital-life-news/world-wide-web-creator-tim-bernerslee-calls-for-a-digital-bill-of-rights-to-ensure-internet-freedom-20140313-34nj3.html.

106 Available at: internetrightsandprinciples.org/site/.

107 Available at: www.apc.org/en/node/5677.

108 See: edri.org/wepromise-whats-point/.

109 Amar Toor, "Cutting the cord: Brazil's bold plan to combat the NSA", *The Verge*, 25 September 2013. Available at: www.theverge.com/2013/9/25/4769534/brazil-to-build-internet-cable-to-avoid-us-nsa-spying.

110 "New Nuclear Sub Is Said to Have Special Eavesdropping Ability", *New York Times*, 20 February 2005. Available at: www.nytimes.com/2005/02/20/politics/20submarine.html?_r=0.

111 Jeanette Seiffert, "Weighing a Schengen zone for Europe's Internet data, *DW*, 20 February 2014. Available at: www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482.

112 Oded Yaron, "Iranians respond to Israeli Facebook initiative: Israel, we love you too", *Haaretz*, 19 March 2012. Available at: www.haaretz.com/news/national/iranians-respond-to-israeli-facebook-initiative-israel-we-love-you-too-1.419505.

113 See map.opennet.net.

114 Available in Portuguese at: www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1238705&filename=Tramitacao-PL+2126/2011.

115 See, for example, Emma Llansó, "Momentum Builds for Brazil's Internet Rights Law", *Center for Democracy and Technology*, 27 September 2013. Available at: cdt.org/momentum-builds-for-brazil's-internet-rights-law/.

116 Angelica Mari, "Brazil gives up on local data storage, demands net neutrality", *ZDNet*, 19 March 2014. Available at: www.zdnet.com/brazil-gives-up-on-local-data-storage-demands-net-neutrality-7000027493/.

117 Hilmar Schmundt and Gerald Traufetter, "Digital Independence: NSA Scandal Boosts German Tech Industry", *Der Spiegel*, 4 February 2014. Available at: www.spiegel.de/international/business/german-it-industry-looks-for-boom-from-snowden-revelations-a-950786.html.

118 H.R.3361.IH, 113th Congress. Available at: thomas.loc.gov/cgi-bin/query/z?c113:H.R.3361:.

119 Kim Zetter, Split the NSA in Two, Says Security Firm Embroiled in NSA Scandal, *Wired*, 25 February 2014. Available at: www.wired.com/threatlevel/2014/02/rsa-head-discusses-nsa/.

120 Kesha West, "Huawei won't bid for large US contracts amid cyber-spying accusations", *Australia Network News*, 5 December 2013. Available at: www.abc.net.au/news/2013-12-05/an-huawei-won27t-bid-for-large-us-contracts-amid-spying-allega/5138210.

121 Nick Sullivan, "How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer", *Ars Technica*, 5 January 2014. Available at: arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/.

122 See www.mozilla.org/en-US/contribute/ for more information about contributing to Mozilla.

123 See www.torproject.org/getinvolved/volunteer.html.en.

124 See: www.spiegel.de/international/business/bild-950786-653221.html.

125 Statistics available at: metrics.torproject.org/users.html?graph=userstats-relay-country&start=2013-06-13&end=2014-03-13&country=all&events=off#userstats-relay-country.

126 James Temple, "Privacy firms boom in wake of surveillance scandal", *San Francisco Gate*, 9 November 2013. Available at: www.sfgate.com/technology/dotcommentary/article/Privacy-firms-boom-in-wake-of-surveillance-scandal-4971062.php.

127 Terje Langeland, "Microsoft to Expand Use of Encryption to Protect Against Spying", *Bloomberg*, 5 December 2013. Available at: www.bloomberg.com/news/2013-12-05/microsoft-to-expand-use-of-encryption-to-protect-against-spying.html.

128 Angelica Mari, "Brazilian postal service talks about "anti-snooping" email system", *ZD Net*, 4 September 2013. Available at: www.zdnet.com/brazilian-postal-service-talks-about-anti-snooping-email-system-7000020257/.

129 "Back to the future: Kremlin buys $15,000 in typewriters to avoid leaks", *Global Post*, 11 July 2013. Available at: www.globalpost.com/dispatch/news/afp/130711/kremlin-turns-back-typewriters-avoid-leaks.

130 "Cracked credibility", *Economist*, 14 September 2013. Available at: www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and.

ACKNOWLEDGEMENTS

This guide was drafted by Michael Karanicolas, Legal Officer, Centre for Law and Democracy, with support and editing by Toby Mendel, Executive Director, Centre for Law and Democracy. Additional research was provided by pro bono students and volunteers Paul Calderhead, Roberto Henriquez, Portia Karegeya, Jane Loyer and Rohan Rajpal. Thanks to Global Partners Digital for their helpful input.

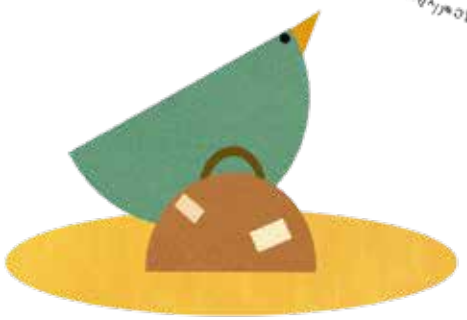
Produced by Tactical Studios
Designed by Miriam Hempel | Illustrations by Valentina Cavallini
Printed in India by Precision Fototype Services, Bangalore

Printed on Fedrigoni Woodstock Betula
FSC accredited paper

The internet has enabled an unprecedented ability to monitor and track people and information flows as highlighted in the 2013 revelations by Edward Snowden about online surveillance carried out by the United States' National Security Agency.

The revelations have kicked off debates across the world about the correct balance between citizen privacy and national security in the context of the internet. In the face of this shifting landscape it is critical for human rights activists to understand how internet surveillance works, and what privacy and anonymity really mean in a digital world.

Surveillance and International Standards is the second in the Travel Guide to the Digital World series, which is designed to assist newcomers to understand, follow and engage in internet policy and governance debates.



ISBN 9780992914714