PRIVACY AND THE MEDIA

ANDREW MCSTAY

SAGE

Los Angeles | London | New Delhi
Singapore | Washington DC | Melbourne

SAGE

Los Angeles | London | New Delhi
Singapore | Washington DC | Melbourne

SAGE Publications Ltd
1 Oliver's Yard
55 City Road
London EC1Y 1SP

SAGE Publications Inc.
2455 Teller Road
Thousand Oaks, California 91320

SAGE Publications India Pvt Ltd
B 1/I 1 Mohan Cooperative Industrial Area
Mathura Road
New Delhi 110 044

SAGE Publications Asia-Pacific Pte Ltd
3 Church Street
#10-04 Samsung Hub
Singapore 049483

Editor: Michael Ainsley
Editorial assistant: John Nightingale
Production editor: Imogen Roome
Copyeditor: Neil Dowden
Proofreader: Jill Birch
Indexer: Adam Pozner
Marketing manager: Lucia Sweet
Cover design: Jennifer Crisp
Typeset by: C&M Digitals (P) Ltd, Chennai, India
Printed in the UK

Library of Congress Control Number: 2017932218

British Library Cataloguing in Publication data

A catalogue record for this book is available from
the British Library

This work was generously supported by the UK's Arts and Humanities Research Council [grant number AH/M006654/1]

ISBN 978-1-4739-2492-5
ISBN 978-1-4739-2493-2 (pbk)

At SAGE we take sustainability seriously. Most of our products are printed in the UK using FSC papers and boards. When we print overseas we ensure sustainable papers are used as measured by the PREPS grading system. We undertake an annual audit to monitor our sustainability.

CONTENTS

4

THE SNOWDEN LEAKS

A CALL FOR BETTER SURVEILLANCE

> In the end we can't be transparent about most of these issues and we have to, get comfortable, with the idea that we are delegating to somebody the ability to learn the secrets, to review what's being done and determine whether it's being done properly. We cannot simply bring everyone in off the street and tell them what is happening.[1] (Stewart Baker, Former National Security Agency (NSA) General Counsel)

> I didn't want to change society. I wanted to give society a chance to determine if it should change itself. All I wanted was for the public to be able to have a say in how they are governed.[2] (Edward Snowden, former NSA employee)

> Traditional, effective surveillance means targeting suspects. Not a population. Not a technology. Not a service. The suspect.[3] (Edward Snowden)

Key questions

- What is the current scope of digital data surveillance?
- What are the problems with mass surveillance?
- Is surveillance effective?
- How can security and intelligence agencies be made more accountable?

Key concepts

- Surveillance
- Chilling effect
- Accountability
- Absolute control (and its impossibility)

In June 2013, Edward Snowden, a US national security whistle-blower, revealed that intelligence agencies in so-called ‘Five Eyes’ nations (Australia, Canada, New Zealand, United Kingdom and the United States) are engaging in secret global surveillance. This comprises bulk data collection, storage and analysis of citizens’ digital communications. Without Snowden it is quite possible that we might never have known about the existence of not just surveillance states, but a surveillance assemblage of states and corporate actors that spans the globe. Where only a few years ago such a sentence would have been cause for ridicule and accusations of tin-foil hat wearing, this is now recognised by critics and governments alike as fact. His actions represent a fundamental shift in what we know about surveillance. Critically it provided evidence of mass surveillance, which is paramount for anyone seeking to factually understand what is taking place. The reach and detail of the Snowden leaks surprised nearly everyone – including computer scientists, privacy scholars and privacy activists. The leaks reveal governments’ indiscriminate data collection, or the ‘grab everything and look through it later if it becomes relevant’ approach. According to the leaks, this includes data from globally significant players such as Microsoft, Yahoo!, Google, Facebook, Pal-talk, YouTube, AOL, Skype and Apple. Revised approaches and legislation about surveillance and data interception began to appear in 2014 in the US and 2015 in the UK.

This chapter opens by outlining the background and consequences of the Snowden leaks and progresses to consider the implications for privacy, particularly in terms of the ‘chilling effect’ of mass surveillance. Although I will summarise the leaks, what data is collected and why this happened, I will not go into detail about the nature of the surveillance programmes. There are a number of sources that do this in a far more engaging manner than can be achieved here. The *Guardian* newspaper has a publicly available multimedia exposition of the Snowden revelations, interviews with key actors and rich explanations of surveillance programmes at a website titled ‘NSA Files: Decoded’.[4.] Please spend time looking through this resource. *The Intercept* also provides readable but in-depth ongoing coverage of the leaks. Also of interest is the Snowden Archives[5] that detail every published leak made by Snowden (note that only a tiny fraction have been published in the press). The filmmaker Laura Poitras also documented events in *Citizenfour* (2014). For further academic sources, see the journal *Surveillance & Society*, especially the 2015 special issue titled ‘Surveillance and Security Intelligence after Snowden’.[6] You might also want to follow Edward Snowden himself on Twitter at @Snowden.

BACKGROUND CONTEXT

Why might the Snowden leaks matter to you? The reader is entirely forgiven for not being able to comprehend the scale of this situation, or possibly the connection with media. To bring this into focus pick up your phone and consider that it is *this* device, that is *your* device, that mediates *your* life, that is having its call, location, searches and internet communications tracked. Note too that surveillance is not applied on us from above, but it is something that works *through* our devices. Importantly too we participated, and continue to do so, in our own surveillance by posting on Facebook, Twitter and beyond, and using services such as Google Docs (Lyon, 2015).

What Snowden revealed is of profound historical importance. Although some of the technologies discussed in this book will undoubtedly not seem as important in five, ten or twenty years' time, Snowden's actions *will* stand the test of time and take their place in the line-up of key events in the early twenty-first century. The significance of what Snowden revealed is that for those of us living in the US, Australia, Canada, New Zealand and the United Kingdom, all forms of our networked communication are potentially being watched by our governments. This changes how we think about media and communication, and what we consider as private and public. In a pre-digital era, only totalitarian countries would trace our mail and record details about our telephone calls (Koehler, 1999). (For an excellent depiction of this, see the 2007 film *The Lives of Others*.) This is now routine in democratic countries. Time will tell whether this is the new normal. The Snowden leaks have forced society to answer some difficult questions because security and intelligence services *do* play a pivotal role in protecting national security and upholding the rule of law.[7] They do this by collecting, analysing and disseminating a wide range of information types, although here we will focus on signals intelligence (interception of data on digital networks).[8] The questions we need to address include: how should we react to governments that wilfully kept secret they were spying on their citizens' communications; what is the balance between rights and societal obligations; to what extent should we accept curbs on our rights in the name of protecting society; how do we decide limits on what should be surveilled; and how are we to have this discussion when the terms of the discussion are secret and/or technically difficult to understand?

I do not want either myself or readers of this chapter to lapse into lazy emotive arguments that depict American, Australian, Canadian, New Zealand and the United Kingdom governments as malevolent or evilly acting against their citizens, but I also urge that readers leave any mention of 'nothing to hide, nothing to fear' at the door for reasons dealt with in Chapter 2. We should also be clear that what is taking place *is* surveillance and that usage of this word is not hyperbole or excessive in any way. It is quite the opposite in that it is a more accurate diagnosis than any other word one might think of. David Lyon, for example, an expert in surveillance studies, says surveillance is 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered' (2001: 2). Another leader of surveillance studies, Gary Marx, defines it as 'the use of technical means to extract or create personal data' (2002: 12). These definitions may appear counter-intuitive: after all, surely surveillance is about tracking suspicious individuals? This has changed and, as this chapter will discuss, *all* people are tracked today to provide a background against which unusual behaviour may be judged. In addition to the extent of surveillance that is taking place, what Snowden showed is that our mediated selves are increasingly visible and transparent, but conversely those who do the watching are very difficult to see, despite the scope of the infrastructure. As highlighted in Chapter 2, this is not the way that democracy was originally conceived. In the US alone, the surveillance assemblage is huge. For example the Utah facility of the National Security Agency (NSA) is a $1.5 billion centre. Employed to collect and analyse data from the internet, the building possesses its own water-treatment facility, uses over a million gallons of water a day, has an electric substation and 60 back-up diesel generators. *The Economist*[9] cites a source saying that its data-storage capacity would be enough to store a year of footage of round-the-clock video recording of over a million people. It achieves its data collection of communications from across the globe by tapping directly into the fibre-optic backbone of the internet.

My point is that the material structure of surveillance is very real, yet we are asked to take on trust that the secrecy (before Snowden) surrounding surveillance by the state is necessary. Historically, democracies have worked the other way around in that we grant the state licence to act on our behalf but we ensure it is accountable to citizenry; and that citizens are free from unwanted inspection as long as they behave in accordance with the law. Snowden revealed that both these principles were broken. Although transparency is a conceptual term, it is one that sits at the heart of what is often posited as the debate between security and liberty, or the question of how much secrecy we should allow the state and its intelligence agencies.

To understand the rise of US-led mass global surveillance, we have to understand something of what took place in September 2001 – the month that the US was attacked by al-Qaeda, the Islamist terrorist group. These were not just physical attacks, but symbolic attacks on globalisation, world trade and the pre-eminent global superpower. This was a co-ordinated spectacle that transfixed the world. The US government reacted quickly and by 13 September US senators had introduced the first version of the USA Patriot Act, which stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. State surveillance has a much older history and one that consistently entails agencies pushing for greater powers, but events post-2001 dramatically extended US surveillance powers and led to the creation of the global, pervasive surveillance programmes that Edward Snowden revealed in June 2013.

THE LEAKS

This section provides an overview of the leaks, but for a more detailed coverage see the *Guardian,*[10] *The Intercept*[11] and ACLU.[12] Although Snowden stole the documents, he did not leak them himself. Instead he worked with Laura

Poitras (a documentary maker) and Glenn Greenwald (a lawyer and journalist) to organise transmission of the documents to a range of news outlets. These include the *Guardian* (Britain), *Der Spiegel* (Germany), *The Washington Post* and *The New York Times* (US), *O Globo* (Brazil), *Le Monde* (France), and other outlets in Sweden, Canada, Italy, Netherlands, Norway, Spain and Australia. Each released edited extracts from the leaks and provided local reporting about their implications. The key revelation from the leaks is that intelligence agencies from the US, Australia, Canada, New Zealand and the United Kingdom routinely collect en masse, and analyse, the communications of their citizens. This includes email, instant messages, the search terms in Google searches, web browsing histories and file transfers. It also includes what is called 'communications data' (in the UK) and 'metadata' (in the USA) (or data about data). Such records of online and mobile activity includes: names, addresses, who is called, call records, length of service, types of service used, number used including temporarily assigned IP address, record of web domains visited, location data of senders and receivers, and means and source of payment. Today, in countries including the UK, the most important metadata may be obtained *without* the permission of a court[13] (Anderson, 2015). This data assists in identifying people of interest, building profiles and contributing to decisions about whether a person should be under targeted surveillance. The attraction of mass surveillance is that information can be collected at a fraction of the cost of tracking through traditional methods. The consequence is that to find suspicious individuals, entire societies are placed under surveillance.

THE PROGRAMMES

Intelligence agencies' mass surveillance relies on global internet and telecommunications companies. This is done by bulk collecting data from companies' servers, and by directly tapping fibre-optic cables carrying internet traffic. It also relies on citizens' own behaviour online as we unwittingly offer up plentiful data about ourselves through our everyday digital communications and digital footprints left across all forms of online activity. The global surveillance apparatus is achieved through several inter-related programmes. These are detailed below.

> *PRISM*: With this programme internet and telecommunications companies were secretly compelled by intelligence agencies in the USA, UK and other liberal democracies to collect and hand over citizens' digital communications. It included tapping into the central servers of leading US internet companies, extracting audio and video chats, photographs, emails, documents and connection logs that enable analysts to track foreign targets (Gellman and Poitras, 2013). Companies that the NSA extracted data from include US service providers Microsoft, Yahoo!, Google, Facebook, PalTalk,[14] AOL, Skype, YouTube and Apple.

UPSTREAM: Whereas PRISM collected data from the servers of US service providers, UPSTREAM is the collection of data traffic as it flows through the fibre-optic cables that comprise the internet.

XKEYSCORE: Disclosed by Glenn Greenwald in an article for the *Guardian*,[15] this is an NSA programme allowing analysts to search databases covering nearly everything a typical user does on the internet, as well as engaging in real-time interception of an individual's internet activity. The leaks showed that the NSA harvests social media activity, browsing history, email, instant messaging contact lists and the location of cell phones. This creates a 'social graph' of individuals' lives in order to identify their associates and search for foreign terrorists, as well as to assemble a person's locations over time. It also piggybacks on cookie data used for advertising and, separately, also attempts to undermine efforts to encrypt communication.

TEMPORA: This is a covert operation by the British government (or what is referred to as 'black-ops'). The surveillance programme is conducted by GCHQ, on behalf of the UK government. It refers to the data interceptors on fibre-optic cables placed by GCHQ that carry internet data in and out of the UK. In operation since 2011, this was done with participation of BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel and Interoute. For sense of context, between 10 and 25 per cent of global internet traffic enters British territory making the UK an important internet traffic hub. TEMPORA stores this data flowing in and out of the UK, sharing it with the USA (Bakir, 2015).

LEGAL COMPLEXITY

One of the most notable features of the leaks is the care that governments have taken to interpret technical and legal frameworks that circumvent national constitutional or human rights protections governing interferences with the right to privacy of communications. Governments have assembled lawyers to provide workarounds and interpretations that are for the most part legal (although as indicated below, they have also overstepped the mark). This is extremely complex and even David Anderson (2015: 8), the independent Queens Counsel (QC) that led the review of the UK's anti-terrorism laws, said that interception laws such as RIPA are obscure and patched up so many times that they are incomprehensible to all but a tiny band of initiates.

In the UK, what is clear is that GCHQ admitted to what were once secret 'arrangements' to accessing bulk material collected by the NSA. This was made public as non-governmental organisations (NGOs) launched a legal challenge against GCHQ's extensive surveillance practices in 2014, arguing that the activities of the government intelligence services breached Articles 8 and 10 of the European Convention on Human Rights (also discussed in Chapter 3). In response to a legal challenge made by Privacy International, Liberty and Amnesty International about international surveillance techniques the government submitted evidence to the Investigatory Powers Tribunal in which it states that obtaining warrants for data isn't necessary in all circumstances. It argued that 'RIPA [Regulation of Investigatory Powers Act] interception warrant is not as a matter of law required in all cases in which unanalysed intercepted communications might be sought from a foreign government',[16] and that the practice doesn't involve 'deliberate circumvention' of RIPA. The consequence of this statement is that any call, internet search or website a person has visited can be stored in GCHQ's database and analysed at will. This can be done without a warrant to collect this information about UK citizens. The US and UK have a reciprocal deal whereby the US collects information about UK citizens, which is then handed back to the UK, so to get around the UK's interception laws.

In addition to penetrating communications networks and companies that run these, governments and their agencies have created complicated legal arrangements that are justified in private by arguments that stretch credulity and arguably break it. The legality is questionable, but the principal problem from a civic point of view is that because people did not know about these practices and legal arrangements, they were unable to challenge it. This is a fundamental point because governments and agencies created a global surveillance infrastructure to monitor citizens in democracies, without informing their citizens. Put otherwise, governments and defence agencies acted without external, public oversight, relying instead on secretive internal oversight mechanisms such as parliamentary or congressional intelligence oversight committees. This removes the public's capacity to challenge intelligence agency's actions: the public cannot hold their governments accountable when actions of key agencies are hidden through secret arrangements and covert legal frameworks.

KNOW IT ALL

Journalist Glenn Greenwald's (2014) book *No Place to Hide* summarises the intention and objective of the NSA surveillance apparatus through a leaked slide that says: 'Collect it All', 'Process it All', 'Exploit it All', 'Partner it All', 'Sniff it All' and 'Know it All'. What Snowden revealed is the wish to gain the fullest picture possible and the belief that harnessing all possible data might actually be useful. Defenders of surveillance argue that it is necessary to collect all available data to provide a background against which suspicious signals can be detected (signal to noise ratio). Mass surveillance and bulk collection of data is justified by saying that the aim is not to treat all citizens as suspects, but to provide a background of normalcy so unusual terrorist activity will stand out. This is a key factor of the story: data about networked behaviour is not collected because everyone is a suspect, but the logic instead is that normal behaviour is required to contextualise abnormal behaviour.

Next, the argument is that if armed with 'all' of the data, agencies are not just able to identify terrorist suspects after an event has happened, but they will be able to *pre-empt* terrorism by means of identifying unusual patterns in information. For what is unusual to be established, a 'usual' is required. This is why police and surveillance organisations feel justified in demanding warrantless access to information held by ISPs, and other large organisations that hold and process our information. What this means is that today surveillance is always on. Surveillance is not just applied on suspicion of wrongdoing as used to be the case, but instead it is a socio-technical perpetual condition that is potentially applied to everybody. As Andrejevic (2013) highlights, it is ubiquitous and the surveillance process itself generates the targets to be pursued. As fully explained in Chapter 9, this is done through machine learning and identification of trends, correlations and standout patterns. This information is both horizontal (everywhere and now) and vertical (chronological), and entails retaining records for as long as legally possible.

The argument made by security and intelligence agencies is that from a security/surveillant point of view, analysts do not know when information may be relevant. What is utterly inconsequential now may provide insight a year down the line as new geo-political/policing events unfold. This is illustrated by a now famous article for the *Huffington Post* from 2013 where Gus Hunt, the ex-CIA Chief Technology Officer, boasted in a presentation given while still in post that, 'It is really very nearly within our grasp to be able to compute on all human generated information'. Moreover, 'The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time' and 'Since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever' (Sledge, 2013). The situation is less about gross display of power, but that politicians and security technologists are impelled by panicked urgency to not miss *anything* and to defend against every eventuality. Further, this is justified at a policy level by the fact that it is machines rather than people doing the watching in the first instance. This is important: GCHQ and the UK government argue that mass electronic collection of personal data is not surveillance because human eyes only see the data when a potential threat is flagged by the system. Pro-privacy groups say that electronic collection and processing of personal data is still mass surveillance. The question is this: is it surveillance if human eyes do not see nearly all of the data? The answer becomes clearer if hypothetically we were to have cameras installed in bathrooms, bedrooms and living areas. It may only be machines examining most of the data, but presumably we would agree it is surveillance?

Quite arguably, the politico-ethical problem of our time is not state malevolence, but anxiety, over-reach, misunderstanding of what is technically possible, and a political desire to collect and interpret everything in the name of protecting citizens from terrorists and criminals. A less forgiving diagnosis says that the state wants the ability to readily identify, and hence target and control, its population, including dissenters. While the stated intention is to prevent risks from actualising, the consequence is a politics of absolute control that runs counter to all political persuasions other than those that seek total control. The problem with this is that even if we put privacy and the ethics of 'interfering' with our media technologies to one side, the idea that processing any and every piece of data will make anybody safer is deeply problematic. First it is impossible to collect and store data on all human behaviour and, second, it is highly inefficient to collecting irrelevant, outdated and incorrect information.

PRO-PRIVACY DOES NOT MEAN ANTI-SURVEILLANCE

Very few people interested in the surveillance debate suggest that there should be no surveillance. Instead pro-privacy campaigners argue there should be targeted surveillance rather than indiscriminate surveillance. As will be developed, in addition to scepticism about the value of 'big data' techniques (explored in Chapter 9), the concern is that there is not enough oversight of how dragnet surveillance is used, and that these powers might be abused. To highlight the possibility that powers developed and assumed to fight terrorism can be abused, in 2015 Big Brother Watch[17] reported that a total of 733,237 requests to access surveillance data were made by the UK police force between 1 January 2012 and 31 December 2014 asking to see the 'who, where and when of any text, email, phone call or web search'. For a country as small as the UK, this is a rather large figure. The total number of 733,237 requests is equivalent to 670 requests a day, 28 requests an hour, or one every two minutes; 92.6 per cent of requests were accepted. What this points to is *mission creep*, where the use of powers granted for one purpose are used for another. While many citizens may be willing to grant access to their communications believing this will help stop atrocities, a question remains whether this civic trust is being abused.

SOME PRACTICALITIES

The wish to collect all of the data all of the time is the mission goal, but it is unclear what is gained by this. This is somewhat exasperating for privacy and intelligence scholars. We are told that surveillance works, but few case studies have been presented. We also have little understanding of what is missed by surveillance (with exception of atrocities) or how many false positives are generated. William Binney for example carried out Signals Intelligence (SIGINT) operations and research for the NSA for 36 years.[18] He argues that while the technologies used for mass surveillance and bulk data collection are powerful and far-reaching, the resulting data swamps human analysts. Today arguing that mass surveillance does not work, he goes as far to say that ‘It is 99 per cent useless’ and even that it ‘costs lives, and has cost lives in Britain because it inundates analysts with too much data’. On presenting his arguments to UK parliament in advance of the Investigatory Powers Bill in 2016, he also claims that security mistakes were made before 9/11 because the US had collected information from the terrorists involved in the attacks, but had not been able to check them because of resources. In a video interview posted by Open Rights Group[19] he argues that bulk collection actually gets in the way of stopping attacks in advance because analysts cannot discern intentions and capabilities. For Binney, excess irrelevant information causes inertia, dysfunction and incapacity to act.

As a privacy and media studies academic, I am not privy to sensitive information about the effectiveness of surveillance, but what Binney did is complicate the over-simplistic narratives of ‘security versus liberty’ and ‘nothing to hide, nothing to fear’ because, in addition to over-reach into citizens’ lives, the fact that so much data is being collected makes the work of the intelligence agencies harder. Having officially managed thousands of analysts during his time at the NSA, he is well placed to judge. The practical problem is the noise to signal ratio, or the proportion of useful information to useless information in any given batch of data. Security agencies are not alone because this is a problem that faces the commercial data-mining industry too in that although they can collect a great deal of information about people, extracting meaningful insights is much harder. One wonders if reallocating resources to human policing, investigative work and building positive relationships within communities might raise effectiveness.

HOW DO THE LEAKS INFORM OUR UNDERSTANDING OF PRIVACY?

In 2013 Robert Hannigan took over the role of head of UK’s GCHQ and used his opening speech to point out that privacy is not an absolute right. He will not find a serious privacy campaigner that disagrees with him, because no one believes that privacy trumps all other considerations. This is because, in a liberal democratic society, privacy is a *qualified* right. As explained in earlier chapters, in the hierarchy of rights, privacy is not an absolute right (unlike for example the right not to be tortured), but it is a right that can be encroached upon if there are other more important interests. The real question is whether GCHQ has a good enough reason for initiating a programme of global surveillance with questionable legality and effectiveness, and whether it should have been able to do so without external oversight. In the modern online era, some access to communications data is required. However, in a democracy, the need for tools to maintain safety has to be balanced with the principle that government should respect the rights of law-abiding citizens to privacy and that there is meaningful oversight of what governments are doing. Contemporary information privacy matters are typically framed in terms of liberty versus security. As we saw in Chapter 2, this is the attempt to balance individual rights with the powers we give to the state. There are multiple problems with this. The first is that few would argue we do not need surveillance. What critics are concerned about is the type of surveillance and whether indiscriminate surveillance of entire populations is necessary, or even a good idea. After all, why not spend money on tracing links between bad people rather than surveilling everyone? This debate is not easily resolved because we simply do not know how many plots are foiled because of application of indiscriminate surveillance. What we do know about, however, are the plots that were successful. Recent attacks in Europe for example show that those involved were already known to security services:

- July 2012: the suspects of the Bulgarian attack in Burgas, Malid Farah (also known as Hussein Hussein) and Hassan al-Haj, are linked to Hezbollah.
- May 2013: Michael Adebolajo and Michael Adebowale who killed an off-duty British soldier were known to British security services.
- May 2014: Mehdi Nemmouche, the gunman who opened fire at the Jewish Museum of Belgium in Brussels had known links with radical Islamists.
- January 2015: Chérif and Saïd Kouachi, the *Charlie Hebdo* gunmen, had criminal records and known links with terrorist organisations.
- February 2015: following release from prison two weeks before, the Danish authorities knew the Copenhagen attacker, Omar el-Hussein, was a potential threat.
- November 2015: intelligence services in France and Belgium knew about attackers' jihadi backgrounds (some had had records identifying them as radicals) and others (at least five) had travelled to fight in Syria and returned to homes in France or Belgium.

This is not proof that indiscriminate surveillance is irrelevant or does not work, but what it does suggest is that there is strong value in monitoring known individuals and that few (if any) perpetrators have no record of suspect activity. What this points to is need for improved policing, co-operation, data sharing across borders, pooling of files and sharing of insights known to security services. The key difference is that this requires better human intelligence of known suspects.

GOOGLING FOR ANTHRAX

Following the revelations by Snowden, the American Civil Liberties Union (ACLU) filed a legal case against the US government over the *chilling effect* of mass surveillance on Americans. Although the chilling effect certainly connects with questions of what we are willing to search and say online, and the ways by which the Snowden leaks have inhibited people's willingness to search for anything they deem sensitive, the term is actually an older one originating in 1952.[20] The 'chilling effect' is based on *inhibition and discouragement* of free speech by individuals and groups due to fear of punishment (such as fines, imprisonment, imposition of civil liability or deprivation of a governmental benefit). The nature of a chilling effect has two factors in that it is an act of deterrence, and when people are deterred we can speak of an activity as being chilled. To push this slightly further, and in a US context, a 'chilling effect occurs when individuals seeking to engage in activity protected by the first amendment are deterred from so doing by governmental regulation not specifically directed at that protected activity' (Schauer, 1978: 693). This means that a person may feel deterred even when the activity they are engaging in is not the one a government seeks to stop. For example, people may feel deterred from innocently Googling their favourite rock band (Anthrax) for fear of being suspected of having an intention to build bombs or engage in biological attacks. This goes beyond searching for music content and digital media to more fundamental political matters of the ability to say what we want without fear of reprisal. In other words, it is about democracy and the right to freedom of expression. In the US this is addressed by the First Amendment to their Constitution that prohibits impediment of freedom of speech.

Research from the US is showing that since the Snowden leaks, there has been a decrease in searches of potentially sensitive terms. A Google Trends study after the Snowden leaks of June 2013 found that people were less likely to search using terms that they believed might 'get them into trouble' or 'embarrass' them with their family, their close friends, or with the US government. They found a drop of 2.2 per cent in traffic for search terms that were rated as 'high government trouble' search terms (Marthews and Tucker, 2014). This is an effect of potential surveillance that inhibits or discourages legitimate behaviour. For example while searches of words such as 'anthrax' dropped in frequency so did words such as 'eating disorder' that clearly has nothing to do with terrorism. The study admits it only examined Google (and people may have moved to other, more privacy-friendly, search engines), but the point is an illustrative one in that it demonstrates the risk-aversion aspect of the chilling effect. Here risk is not about what is clear and known, but uncertainty, what-ifs and lack of confidence in the surveillance assemblage to differentiate between an innocent and threatening search query. The Google Trends study also connects with a report from PEN America (2013)[21] that highlights self-censorship of writers in the US after the Snowden leaks. It states that 16 per cent of writers polled by PEN said they would not do certain Google searches in case it piques the government's interest. Twenty-five per cent say they regularly self-censor in email and on the phone. Many are less willing to write about certain topics that includes military affairs, the Middle East and North Africa regions, mass incarceration, drug policies, pornography, the study of certain languages and criticism of the US government. This is understandable because, for example, UK journalists and even comedians have been placed under surveillance and listed as 'domestic extremists'.[22] Similarly, the critical online news publication *The Intercept* has been engaged in a Freedom of Information battle with the UK's Metropolitan Police Service to find out if it is investigating journalists. In July 2015 the police confirmed that they are.[23]

This invokes another characteristic of the chilling effect in that when daunted by the fear of punishment, people may refrain from saying, studying or publishing that which they lawfully should be able to. In times of social uncertainty, this is exactly when authors *should* feel free to express criticism, controversial opinions and assess uncomfortable subject matter (such as videos produced by ISIS/Daesh). To clarify, the problem is that democracy is undermined because citizens are fearful of voicing dissenting opinions in public, or even finding out more about what is taking place. In 2016 other US research demonstrated that the NSA's capacity to monitor the online activities of US citizens 'can contribute to the silencing of minority views that provide the bedrock of democratic discourse' (Stoycheff, 2016: 1). What this means is that majority opinion is able to dominate without challenge, but also that the majority is able to take control of online spaces (such as Facebook and other social media) where discussion and deliberation takes place. Inhibition and the chilling effect thus does not just impact on individuals who feel dissuaded, but society, as authors, academics and journalists worry about reprisal. The fear of reprisal is exacerbated by uncertainty, particularly when we know what we are doing is legal, but we fear that surveillers will come to another conclusion about our actions and motives. In the case of electronic surveillance this is intensified by: reach of the aforementioned security programmes; mistrust in the effectiveness of machinic analysis of key words that do not take into account context and motive (false positives and misidentification of threats); and direct fear of dissent from governmental arguments (as in the George W. Bush aphorism, 'if you're not with us, you're against us').

CONCLUSION

This chapter has outlined some of the privacy implications of the Snowden leaks of 2013. Having detailed the background context to the leaks and presented an overview of what information is being collected, it progressed to consider the effectiveness of surveillance and the social effects. Due to the fact that so little is published about its effectiveness, it is difficult to make the case for mass surveillance. What we do know, however, is that perpetrators of atrocities are typically already known to security agencies, which calls into question the need to monitor the communications of entire populations. This point perhaps becomes more convincing if we consider the testimony of William Binney, the ex-NSA employee of 36 years turned whistle-blower, who argues that the data presented by bulk data collection makes the work of analysts harder, and hinders comprehension of a target's intentions and capabilities. He even goes as far to suggest that mass surveillance has cost lives. If Binney is right, far more preferable is greater reliance on community and human intelligence, rather than big data processing (and its generation of false positives that tie-up analysts). One might respond that we need better mass surveillance, but the onus is then to answer how much is enough, where is the line, what are the limits and what forms of oversight should we have. This is perhaps the biggest surprise from the Snowden leaks: that oversight of mass surveillance activities and accountability to the public has been so sorely missing.

Although the connection between privacy, surveillance, media and personal technologies is self-evident, this chapter has focused on the chilling effects of mass surveillance. This is when people feel inhibited to speak publicly, and in our case use media technologies to search for information. The principle of chilling effects has legal origins in the US and the 1950s. It is less a direct threat than a vague fear of reprisal, potential negative outcomes, incursion of further monitoring and a risk-based decision to desist from a line of action. In our case, this is a decision not to search for information through a search engine we know to have been under surveillance by national security agencies. This inhibition and discouragement is pervasive and has risen since Snowden's disclosures. This is deeply undesirable because a person will feel deterred even when they are not doing anything wrong. The net result of this is distrust of the web, a sense of being out of control (low privacy), lack of willingness of citizens to research and inform themselves, and even avoidance of reading up about personal matters unrelated to terrorism.

Research and challenges

1. This chapter has only begun to detail the extent and nature of contemporary surveillance activities. Explore the sources given early in this chapter and also find two more high quality sources about modern surveillance. Discuss points of interest with your peers.
2. How satisfactory do you find the premise that mass surveillance is necessary to create a backdrop against which deviancy might be discerned. What are the problems with this, if any?
3. Is it mass surveillance if human eyes do not see most of the data collected? Explore both sides of the argument and come to a conclusion.
4. Governments and their security agencies should be accountable to citizens but a degree of secrecy is necessary for these agencies to function effectively. How can accountability and meaningful oversight be built in? Also see David Anderson's report for the UK government, *A Question of Trust*. This is available online.

NOTES

[1] Audio file available from www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[2] Available from www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

3 Available from: https://twitter.com/snowden/status/659408231794610176?lang=en-gb.

4 Available from www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

5 Available from https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cg

6 Available from http://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/Intelligence.

7 Intelligence services have a foreign mandate and focus on external threats while security services have a domestic mandate and focus on domestic threats.

8 The Federal Bureau of Investigation (FBI) has a useful list intelligence types available at www.fbi.gov/about-us/intelligence/disciplines.

9 Article available from www.economist.com/news/united-states/21651817-america-argues-anew-over-how-much-snooping-nsa-can-do-reviewing-surveillance-state?frsc=dg%7Cd.

10 See www.theguardian.com/us-news/the-nsa-files.

11 See https://theintercept.com/search/?s=snowden.

12 See www.aclu.org/nsa-documents-search.

13 Note, however, that in Canada and Australia, some form of judicial authorisation is required before the police may access metadata. In the US, the FBI may access metadata without judicial authorisation, but state police forces ordinarily require a subpoena or a court order in order to do so (Anderson, 2015).

14 This is a chat and instant messaging service.

15 Article available from www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

16 Quote available at www.theguardian.com/uk-news/2014/oct/29/gchq-nsa-data-surveillance?CMP=EMCNEWEML6619I2.

17 Big Brother watch available from www.bigbrotherwatch.org.uk/wp-content/uploads/2015/05/Big-Brother-Watch-Report-Police-Communications-Data1.pdf.

18 William Binney worked for the NSA for 36 years and oversaw the development and construction of the first technologies used for the bulk collection of Internet communications. He left the NSA after the 9/11 attacks when the agency greatly expanded its surveillance programmes and began surveilling the US population.

19 Available from www.youtube.com/watch?v=Xeo1e_T_USI.

20 The United States Supreme Court first uses the term in the context of the United States Constitution in *Wieman v. Updegraff* [1952]

21 PEN America is a fellowship of writers, editors and translators that works to advance literature and defend free expression.

22 See the article from the British newspaper the *Independent* that highlights that a number of journalists and the comedian Mark Thomas were placed on watch lists: www.independent.co.uk/news/uk/crime/six-journalists-sue-the-british-police-over-spying-revelations-9874795.html.

23 Letter of confirmation from the police force at: https://s3.amazonaws.com/s3.documentcloud.org/documents/2178930/uk-met-police-snowden-investigation-foi-response.pdf.