idea as others of what metadata or algorithms are, but they will discover all too sharply in practice what it means to be singled out as a person-of-interest.

All this raises further questions: What are the prospects for privacy in the twenty-first century? Does the concept of privacy encompass all that is challenged – or even threatened – by what we now know about state surveillance, following Snowden? And, when persons of interest concern themselves about privacy, how does this relate to their concerns about civil liberties and human rights – or even about democracy itself? It is these questions that we have to address if we are to complete our analysis of surveillance after Snowden.

# 4

# PRECARIOUS PRIVACY

Your rights matter because you never know when you're going to need them.

Edward Snowden, March 2014

Let me tell you about Faisal Gill. He is a patriotic American, a Republican, served in the Navy, had high-level security clearance when he worked for the Department of Homeland Security under George W. Bush, works in his community, sent his children to a Catholic school, is a lawyer. It was revealed by Edward Snowden through Glenn Greenwald on 9 July 2014 that the NSA and the FBI have been covertly monitoring his emails under secretive procedures intended to target terrorists and foreign spies.[1]

Why? He is a Muslim. As it turns out, this has happened to many other prominent American Muslims. As reported in 2011, the FBI teaches its operatives that 'mainstream Muslims' are 'violent, radical'.[2] Faisal Gill's story is just one

of many that has come to light thanks to Snowden. It raises questions about how these things happen – the Foreign Intelligence Surveillance Act was supposed to limit McCarthy-like witch-hunt excesses after 9/11 – about access to electronic communication, including emails and social media, by police, security and intelligence agencies. It also throws down a gauntlet about privacy rights, democracy and dignity.

This case is important because it shows that not only is Faisal Gill susceptible to surveillance, like anyone else within sight of the NSA, but he is also in a group singled out for special scrutiny, as an American Muslim. Thus his rights to privacy have not only been diminished along with millions of others, but they are, apparently, different from those in other groups. He was deeply disturbed to discover that he was being surveilled because he is fully aware that part of what it means to live in a democracy is to know what the government is doing and to have the chance to question it, if necessary.

The word privacy appears with great frequency among those who question the appropriateness of what the NSA and its partners do. Privacy unites a variety of oppositional figures of all political stripes in a post-Snowden world. This chapter explores what is meant by privacy and why it is indispensable. Privacy is a pivotal concept that helps to throw light on what is wrong with mass surveillance and there are many levels on which it can be used for this purpose. Privacy is also closely connected with other categories of complaint against mass surveillance, including rights such as freedom of association, speech, religion, conscience, movement – rights that are basic to democratic ways of organizing society.

Snowden's own comments certainly point to privacy as a vital value and one that should be maintained by more than one means. Speaking in June 2014 on the first anniversary of the initial leaks, for example, he said that users should seize



privacy, 'take back the net', by adopting encryption for their computers and digital devices. But he also argued for using political means – voting for those who would limit unnecessary and illegal surveillance, as a way of combating mass surveillance of the kind that his work has revealed.[3] More broadly still, he often speaks of the need to eliminate mass surveillance as something that is incompatible with democratic practices. In this broader sweep, there are cases such as that of Faisal Gill. Post-Snowden politics also speaks to his situation. How do we square specific surveillance of Gill and his family, simply because they are Muslim, with living in a fair and just society?

This chapter starts out with privacy as conventionally construed, and then moves out to think of privacy in several different dimensions. The chapter concludes by discussing the extent to which mass surveillance should even be contemplated in societies that lay claim to being democratic. The twist in the tail is the question of whether societies that permit mass surveillance and put pressure on privacy are actually undermining the very possibility of politics.

## Privacy Asserted: The Back-Story

Wherever there is pervasive state-initiated surveillance, the same questions have to be asked. Privacy is under threat in new ways. How this is perceived varies from country to country but most agree that there is personal and social benefit from having a realm where people can think, write, talk, play or generally 'be themselves' away from the eyes and ears of others, especially those in authority. Privacy is often seen as having a number of dimensions: the choice to be let alone – 'unhindered', that is – limiting others' access to the self, and rights to secrecy, control of personal information,

of many that has come to light thanks to Snowden. It raises questions about how these things happen – the Foreign Intelligence Surveillance Act was supposed to limit McCarthy-like witch-hunt excesses after 9/11 – about access to electronic communication, including emails and social media, by police, security and intelligence agencies. It also throws down a gauntlet about privacy rights, democracy and dignity.

This case is important because it shows that not only is Faisal Gill susceptible to surveillance, like anyone else within sight of the NSA, but he is also in a group singled out for special scrutiny, as an American Muslim. Thus his rights to privacy have not only been diminished along with millions of others, but they are, apparently, different from those in other groups. He was deeply disturbed to discover that he was being surveilled because he is fully aware that part of what it means to live in a democracy is to know what the government is doing and to have the chance to question it, if necessary.

The word privacy appears with great frequency among those who question the appropriateness of what the NSA and its partners do. Privacy unites a variety of oppositional figures of all political stripes in a post-Snowden world. This chapter explores what is meant by privacy and why it is indispensable. Privacy is a pivotal concept that helps to throw light on what is wrong with mass surveillance and there are many levels on which it can be used for this purpose. Privacy is also closely connected with other categories of complaint against mass surveillance, including rights such as freedom of association, speech, religion, conscience, movement – rights that are basic to democratic ways of organizing society.

Snowden's own comments certainly point to privacy as a vital value and one that should be maintained by more than one means. Speaking in June 2014 on the first anniversary of the initial leaks, for example, he said that users should seize



privacy, 'take back the net', by adopting encryption for their computers and digital devices. But he also argued for using political means – voting for those who would limit unnecessary and illegal surveillance, as a way of combating mass surveillance of the kind that his work has revealed.[3] More broadly still, he often speaks of the need to eliminate mass surveillance as something that is incompatible with democratic practices. In this broader sweep, there are cases such as that of Faisal Gill. Post-Snowden politics also speaks to his situation. How do we square specific surveillance of Gill and his family, simply because they are Muslim, with living in a fair and just society?

This chapter starts out with privacy as conventionally construed, and then moves out to think of privacy in several different dimensions. The chapter concludes by discussing the extent to which mass surveillance should even be contemplated in societies that lay claim to being democratic. The twist in the tail is the question of whether societies that permit mass surveillance and put pressure on privacy are actually undermining the very possibility of politics.

## Privacy Asserted: The Back-Story

Wherever there is pervasive state-initiated surveillance, the same questions have to be asked. Privacy is under threat in new ways. How this is perceived varies from country to country but most agree that there is personal and social benefit from having a realm where people can think, write, talk, play or generally 'be themselves' away from the eyes and ears of others, especially those in authority. Privacy is often seen as having a number of dimensions: the choice to be let alone – 'unhindered', that is – limiting others' access to the self, and rights to secrecy, control of personal information,

of many that has come to light thanks to Snowden. It raises questions about how these things happen – the Foreign Intelligence Surveillance Act was supposed to limit McCarthy-like witch-hunt excesses after 9/11 – about access to electronic communication, including emails and social media, by police, security and intelligence agencies. It also throws down a gauntlet about privacy rights, democracy and dignity.

This case is important because it shows that not only is Faisal Gill susceptible to surveillance, like anyone else within sight of the NSA, but he is also in a group singled out for special scrutiny, as an American Muslim. Thus his rights to privacy have not only been diminished along with millions of others, but they are, apparently, different from those in other groups. He was deeply disturbed to discover that he was being surveilled because he is fully aware that part of what it means to live in a democracy is to know what the government is doing and to have the chance to question it, if necessary.

The word privacy appears with great frequency among those who question the appropriateness of what the NSA and its partners do. Privacy unites a variety of oppositional figures of all political stripes in a post-Snowden world. This chapter explores what is meant by privacy and why it is indispensable. Privacy is a pivotal concept that helps to throw light on what is wrong with mass surveillance and there are many levels on which it can be used for this purpose. Privacy is also closely connected with other categories of complaint against mass surveillance, including rights such as freedom of association, speech, religion, conscience, movement – rights that are basic to democratic ways of organizing society.

Snowden's own comments certainly point to privacy as a vital value and one that should be maintained by more than one means. Speaking in June 2014 on the first anniversary of the initial leaks, for example, he said that users should seize



privacy, 'take back the net', by adopting encryption for their computers and digital devices. But he also argued for using political means – voting for those who would limit unnecessary and illegal surveillance, as a way of combating mass surveillance of the kind that his work has revealed.[3] More broadly still, he often speaks of the need to eliminate mass surveillance as something that is incompatible with democratic practices. In this broader sweep, there are cases such as that of Faisal Gill. Post-Snowden politics also speaks to his situation. How do we square specific surveillance of Gill and his family, simply because they are Muslim, with living in a fair and just society?

This chapter starts out with privacy as conventionally construed, and then moves out to think of privacy in several different dimensions. The chapter concludes by discussing the extent to which mass surveillance should even be contemplated in societies that lay claim to being democratic. The twist in the tail is the question of whether societies that permit mass surveillance and put pressure on privacy are actually undermining the very possibility of politics.

## Privacy Asserted: The Back-Story

Wherever there is pervasive state-initiated surveillance, the same questions have to be asked. Privacy is under threat in new ways. How this is perceived varies from country to country but most agree that there is personal and social benefit from having a realm where people can think, write, talk, play or generally 'be themselves' away from the eyes and ears of others, especially those in authority. Privacy is often seen as having a number of dimensions: the choice to be let alone – 'unhindered', that is – limiting others' access to the self, and rights to secrecy, control of personal information,

personhood and intimacy.[4] But these interpretations vary widely, especially beyond Western countries that often seem to focus on individual rather than collective values.

Privacy is generally regarded as a 'right' or a 'civil liberty' associated with being a free person. The UN High Commissioner for Human Rights reminded us in 2014, for example, that 'surveillance threatens individual rights – including to privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society'.[5] The attacks of 9/11 provoked much interest in privacy around the world after national security policies were enacted that frequently infringed 'informational privacy'. Personal data were crossing borders faster, more frequently, and with fewer controls than before. A key problem is that, typically, information privacy is often seen in law as less important than bodily or territorial privacy.

Yet, as the Snowden revelations show, facial images (body) or location data (territory) are often collapsed into a more bland general category of information relating to persons or groups. Privacy is also connected with living in a democratic society, where there are statutory limits to what government may do secretly, and where we should be able to disagree with the government without fearing the consequences. Why should any democratic government record someone's opposition to anything from abortion and euthanasia to oil pipelines, factory farms or mines run from abroad and supported by foreign governments?

Why are privacy rights and democracy challenged by surveillance today? Both have been achieved only through long struggle and both are fragile and vulnerable. Like beautiful pottery, these things are easier to break than to mend. So how exactly does the surveillance which has been revealed threaten to crack open or break up privacy rights and democracy? And can we even talk about these in the same way in a



digital, 'big data' era? In the northern hemisphere, with ripple effects around the world, 9/11 unleashed many challenges to privacy.[6] The anti-terrorist laws that permitted this were – sometimes – publicly debated, but the agencies that carried them out tend to be highly secretive. The Snowden revelations show just what kinds of things happen behind the closed and heavily guarded doors of the NSA and similar organizations.

We have known since the 1960s about the tendency of police departments in North America, Europe and elsewhere to keep more and more population groups under surveillance, and since the 1970s that, in the name of national security, intelligence and communications agencies were doing the same.[7] Since the 1980s a number of researchers have shown that this trend has been massively amplified by computerization.[8] Note three things:

One, information and risk are central: By the 1990s policing and security was increasingly *defined* in terms of information-handling and its rationale was to manage risks.[9] So the threats to privacy, rights and democracy after 9/11 came as no surprise, although public opposition to these trends never seemed strong or sustained, at least in North America. With the Snowden disclosures, a new and dramatic opportunity to respond to these challenges is presented. The evidence of international mass surveillance of the everyday lives of ordinary citizens grows with each new revelation.

Two, everyone is targeted: It is now widely known that mass surveillance means that 'innocent bystanders' are included in the NSA's surveillance net, both Americans and citizens of many other countries – nine out of ten NSA communications touch innocent people like these.[10] The colossal collection, storage and analysis of personal data – much of which seems trivial, fragmented, inconsequential – from numerous sources is much more difficult to pin down or even

to see as an issue. In fact, as we have seen, privacy is everyone's problem.

Three, individuals are 'made up': Mass surveillance uses data in new ways that disconnect the data from the individual – I call it 'personal data without the person' – but the profiles created from such data gathering are often misleading, irrelevant and damaging to specific individuals or groups. The ways in which people are 'made up' by the data in these impersonal systems are far from incidental in the real flesh-and-blood lives of those people.

## Privacy Versus Surveillance

Privacy then, is a vital part of the Snowden story. Glenn Greenwald, for example, points out that when government or business says privacy is less important today, individual spokespersons do not believe what they themselves say. In the US, when Senator Dianne Feinstein asserted the NSA's collection of metadata is not surveillance, online protesters demanded that she publish a monthly list of people she called and emailed, with details of where she was and how long she was in touch. It was inconceivable that she would agree, says Greenwald, because it was a 'clear breach of the private realm'.[11] True enough.

This is typical of the way that the concept of privacy is invoked as an antidote to surveillance. The concept is made to do much work – often with considerable success – in mobilizing the assessment of, and limits to, surveillance. But in order to explore privacy as a means of resisting increasing government surveillance – especially mass surveillance – much more has to be considered than what Senator Feinstein might not want to be revealed in a public inventory of her email and phone communications and personal itinerary, as



Greenwald would be the first to agree. The Snowden revelations are about government surveillance of ordinary citizens, often in the name of national security, that goes well beyond the generally accepted targeted monitoring of those whom policing and intelligence agencies have reason to believe are a direct threat.

Snowden has pulled back the curtain on some huge surveillance secrets. Telephone and internet companies are implicated. The Dishfire program makes it possible for the NSA to scan 200 million text messages of US citizens each day. The NSA spies on world leaders – 122 of them according to *Der Spiegel* – often using their cellphones. It also intercepts phone calls across whole countries, such as Afghanistan, using a program called Mystic to 'replay' conversations from the past.[12] The NSA weakens the security of the internet by cracking or circumventing attempts at encryption. The NSA's TAO – Tailored Access Operations – hacks the internet worldwide and injects malware into the system.[13]

Hardly surprising that 'privacy' appears with such frequency in outraged denunciations of the NSA. Citizens of not only the US but also of many other countries around the world know that their private calls, texts, internet surfing and emails are subject to scrutiny by the NSA and its partners. But the debates occur differently in different countries and opinion polls show considerable variations in public views of what privacy is, why it might be important and whether it may have to be 'traded' for more security at certain times of crisis. With the rise of social media, a further question is added to the mix: does privacy really matter any more when all kinds of personal information and images are voluntarily shared online? Knowing what is meant by privacy is vital if we are to work out what the appropriate responses to Snowden's revelations are.

For example, an international poll taken in 2014 showed that, around the world, 64 per cent of respondents are more concerned about online privacy than in 2013.[14] At 46 per cent Sweden had the lowest rise in the rate of concern about privacy since Snowden's revelations, compared with 62 per cent in the United States. Increased concern about privacy was much more marked in Brazil, India and Nigeria, which each registered at 83 per cent. Although Americans also worry about the security of their information on the internet (only 31 per cent said it is secure), only 36 per cent have done anything to improve their privacy, compared to 69 per cent of Indian respondents.

Such international variations are important, reflecting different levels of dependence on the internet, among other things. While 77 per cent of Americans think that access to the internet is a basic human right, more than 90 per cent of respondents from China, Egypt, Indonesia, Nigeria and Tunisia say so. However widespread the agreement that much is wrong with the way that the NSA operates – this would be one good explanation of the increased concern about privacy – responses to privacy issues vary considerably around the world. And even when people say that they are concerned they do not necessarily attempt to do anything about it.

## Why Privacy Matters

Privacy matters both as a vital value in itself and also for other practices that it supports – such as democracy. It is a robust way of questioning the growth of surveillance, and is undoubtedly the most widely used platform for mobilizing opposition to unnecessary and especially mass surveillance. The fact that it can all too easily be reduced to an individualistic level by



both its supporters *and* its detractors is not an argument for abandoning it. It is rather a challenge to show in what ways privacy is a social and a public good. Nor is the fact that it is historically and culturally relative, or that some languages, such as Japanese or even French, have no single word that corresponds to the English 'privacy', sufficient reason for dropping the term. To the contrary, it is a reason for showing how context is always crucial. 'Privacy' does not speak equally clearly to all aspects of what is wrong with some forms of surveillance. But this is an argument for finding supplementary ways of querying surveillance, not for letting go of privacy.

Space does not permit a full discussion of these matters, especially the critique of inadequate ways of defining privacy.[15] As one who was once known for some fairly severe strictures against privacy, I should say that over the past decade two things have influenced my altered position. One is that as surveillance issues have become more urgent, the need to find common ground for opposition to its negative features has become a priority. And the other is that definitions of privacy are turning from abstract, individualistic and sometimes elitist emphases to much more welcome ones that accent our everyday embodied lives in their relational dimensions. Privacy is part of the common good.

Firstly, privacy is a matter of public policy and, as such, is now often couched in terms of its social and societal benefits, on both sides of the Atlantic and beyond. Most privacy and data protection laws were created precisely because computerization increasingly meant that issues of personal information-handling could not be limited to extraordinary or occasional events. People using credit cards or social insurance numbers in the first instance, and then anyone using digital devices, were more and more vulnerable to system errors, fraud, security breaches – or to direct unauthorized

or secondary use of their personal data. Privacy policy speaks to these matters of public importance – all the more so when the surveillance is done by government agencies like the NSA and its partners without specific warrant and with little or nothing by way of transparency or accountability.

Secondly, privacy never exists in a vacuum. Context makes a difference to what is considered private and this has never been more true than in a day of widespread online communications.[16] The mere fact that many social media users post freely and frequently does not necessarily indicate a lack of interest in privacy so much as a nuanced understanding of what should be confidential or anonymous or protected in varying settings. Young people in Canada, for example, are very clear about the need for limits to the circulation of their posts and, especially, their photos. And while they might think that under some circumstances the police should be allowed to gain access to their data, others, such as teachers, should certainly not be able to see their social media pages.[17] What this means is that privacy regulation should be flexible enough to address such variations while still remaining clear that certain kinds of surveillance are simply unacceptable.[18]

Thirdly, while privacy may not address all aspects of surveillance, privacy policies are constantly being developed to try to ensure that they remain relevant. For example, privacy may be inadequately construed as creating a bubble around the individual, a barrier that should not be transgressed. But as political scientist Colin Bennett points out, most privacy thinkers and policy-makers today recognize that we all *already have* extensive relationships with organizations that handle personal data.

So the question is not so much about privacy as some line in the sand, but rather how those relationships are managed and the extent to which we can trust organizations to take every care of the data while they are in their systems.[19] Which



was exactly what prompted such a scandal when Snowden revealed that phone and internet companies were working with the NSA. Trust between individuals and organizations is fractured when information collected for one purpose and supposedly protected from prying eyes is in fact in use by another, secretive and less than accountable agency.

To take Bennett's argument one stage further, the key reason for seeing privacy as an important value is that it sees human beings as relational. Privacy thought of in individualist terms falls woefully short. Being relational is basic to being human.[20] As Catherine Fieschi says, for humans to thrive, their 'interdependence entailing knowledge of each other and various forms of trust' are essential.[21] German sociologist Georg Simmel pointed out – at the start of the twentieth century – that how we relate to others depends deeply on what we know, and do not know, about them.[22] In this case, too, privacy is connected with an ethics of care for the other. Interdependence and trust assumes care.

In short, privacy as a value is essential. More may be needed but not less than privacy. The concept does mobilize regulation and action and contributes to the common good. Privacy is an essential component of democracy and of a decent human life. At times it has been narrowly conceived as an abstract disembodied ideal, which fails to do justice to the real-life situations to which it in fact refers.[23] It has been criticized for emphasizing the spatial dimension and neglecting social justice aspects of surveillance such as social sorting. Fault has been found when it is reduced to 'information control' rather than being seen in a broader context of rights. It is historically and culturally relative. And today, the concept is also changing in a digital era, which raises further questions about how to retain its effectiveness. But in no way do these things simply or completely add up to a case against privacy.

Privacy is thus the right place to start, simply because in its emerging form it has the capacity to frame opposition to excessive or unwarranted surveillance. Debates over privacy, in this view, foster political, policy and practical change. As privacy expert Valerie Steeves says, 'narrower conceptions of privacy are being displaced by more empowering discourses from a human rights model that protects human dignity and democratic freedoms'.[24] It is vital to work with those who take this view[25] because they are fully aware of the need both to limit surveillance and to work within the parameters of a concept – privacy – that has served that end in public policy for many decades.

## Whistleblowers, Journalists and Other Targets

Some Snowden documents released early in 2015 show that emails from journalists from the BBC, Reuters, *The Guardian*, the *New York Times*, *Le Monde*, *The Sun*, NBC and the *Washington Post* were scooped up in 2008 by GCHQ.[26] Apparently a new tool for stripping irrelevant material from emails was under test. Documents also draw attention to the fact that investigative journalists are seen as a threat alongside terrorists and hackers. One restricted document intended for army intelligence officials observes that 'journalists and reporters representing all types of news media represent a potential threat to security'.

In the UK, more than a hundred editors of newspapers and other news media signed a letter to Prime Minister David Cameron protesting this snooping on journalists' communications.[27] More general opposition to NSA interception and analysis of journalists' and others' communications has occurred in various places in Europe and the US – such as 'Restore the Fourth', meaning the Fourth



Amendment of the American Constitution, on the annual Fourth of July Independence Day. Such resistance to the curtailing of civil liberties makes sense, given the direct challenge to human rights. A democracy depends directly on a free press.

An important outcome of the Snowden revelations was to prompt President Obama to commission a report by the President's Review Group on Intelligence and Communications Technologies, published as *The NSA Report: Liberty and Security in a Changing World* (2014).[28] Significantly, this report speaks of both privacy and civil liberties, which connects directly with human rights. The authors are clear that 'the current storage by the government of bulk metadata creates potential risks to public trust, personal privacy and civil liberty'.[29] They explicitly state that the rights to freedom and civil liberties that may be threatened online go well beyond privacy. As we have seen, post-Snowden calls for human rights have also been heard in the UN General Assembly, in a speech given in 2013 by Brazilian President Dilma Rousseff.

So privacy itself may be thought of as a right, but other rights – to speak out, to dissent, even to dig below the surface as a reporter – may also be at issue when one is fearful that conversations are being monitored by the NSA or any other agency. Article 12 of the Universal Declaration of Human Rights asserts that our reputation should not be impugned, our homes entered or our correspondence intercepted without good reason.

On 16 July 2014 the UN High Commissioner for Human Rights spoke out against the 'disturbing lack of transparency about government surveillance…' that causes human rights violations.[30] But article 19 of the Universal Declaration also speaks to the Snowden affair: the right to freedom of expression. Free speech is also jeopardized by mass surveillance.

Privacy is for all. But the other rights at stake give even more reasons for opposing excessive, unwarranted and illegal surveillance. And seeking privacy as a right may help to bolster those rights as well.

Over the past two decades, it has become increasingly clear that surveillance is unevenly distributed. That is, some population groups find themselves under more intensive scrutiny than others, or because the data are processed in particular ways, some groups are unjustly discriminated against. Since 9/11, for example, airport security checks in North America, Europe and elsewhere have resulted in disproportionate delays and detainment for brown-skinned people, especially if they appear to have 'Muslim' or 'Arab' features or profiles. Recall the Faisal Gill example. As well, already marginalized groups such as African Americans in the US, refugees from the global south in Europe, or the poor – anywhere – also find that they are singled out for further disadvantage whether through the surveillance mechanisms of welfare or credit-ratings.[31]

The Snowden revelations themselves show the extent of government attempts to stifle popular protest and political dissent. I noted earlier the collaboration between the Canadian CSE and the NSA to monitor the G8 and G20 meetings in 2010. The secret surveillance of the summit meetings included scanning for possible 'troublemakers' who might be making their way to Toronto by rail or road and whose activities could be tracked as they arrived. An 'internet monitoring unit' was deployed by the Royal Canadian Mounted Police (the federal police), for instance, although it is hard to discover exactly how this worked. Equally, how judgements were made about the identity of 'troublemakers' is unclear. What is clear, however, is that more carefully restricted surveillance practices would help to prevent the predictable scenes that ensued.[32]



The protests at the G20 in Toronto were notorious for the TV images of gratuitous street violence by some, and also by police – leading to calls for a public inquiry from Amnesty International and complaints about brutality from well-respected figures.[33] A student friend of mine attending a prayer vigil at the protests was arrested and fined heavily on the grounds that the pocket knife he carried in his backpack to cut fruit for the group was a 'dangerous weapon'. The aim of the authorities was clearly to intimidate any who wished to express their views – whether to God or to fellow citizens – publicly.

So it is vital to pursue a rights-based approach to surveillance that acknowledges privacy as a value to be maintained for all, but also one to be stressed in relation to those who face unfair discrimination through the targeting of 'suspect' groups – the social sorting of surveillance. Privacy is a springboard into these broader issues. Rights-based approaches are important and belong alongside others, such as a critical ethics of care.[34] If there are rights to fair treatment, there are also rights to express oneself, even to go out on a limb if the situation calls for it. The question of protest, dissent and whistleblowing raises further issues, that also prompt questions about surveillance and democracy.

Since Snowden, it has become even more apparent in many countries that dissenters, protesters, whistleblowers and indeed anyone who criticizes government and corporate power is likely to come under special scrutiny. Snowden himself provides a case in point. It was only after he could find no internal support for his complaints about illegal practices within the NSA that he decided on civil disobedience. Seeing the attacks on and accusations against other whistleblowers in the US – from Daniel Ellsberg of Pentagon Papers fame, to William Binney or Thomas Drake, who also exposed NSA activities – he chose to share his

findings with journalists and to seek safe haven outside the US.

Snowden chose not to speak out as a whistleblower and allow the news to be picked up by the media. Instead, he contacted filmmaker Laura Poitras and investigative journalist Glenn Greenwald and invited them to participate in the process. Journalists were thus involved and in a sense implicated in the revelations. *The Guardian* (UK) and the *Washington Post* (US) actually broke the news but other papers, including the *South China Morning Post* (Hong Kong), *Der Spiegel* (Germany), *O Globo* (Brazil), *L'Espresso* (Italy) and the *New York Times* (US), have also played a role.

However, elements in the mass media also succeeded in casting slurs on Snowden from the start, smearing him as a traitor or worse. The government clampdown on the press that often keeps ordinary citizens from full awareness of other important news worked overtime to dismiss Snowden or deflect attention from the significance of his act. Even the *New York Times*, which seemed fairly even-handed in its Snowden coverage, took until New Year's Day 2014 to declare that 'whistleblower' is the correct descriptor for him and to state unequivocally that he should be given the 'hope of a life advocating for privacy and far stronger oversight of the runaway intelligence community'.[35]

Several other aspects of this should be highlighted. The fear of retaliation in a world of information control is strong. Increased government surveillance may at certain times create chilling effects and self-censorship. A striking instance of this appeared in a survey of American writers by PEN in 2013 that showed how, following the Snowden disclosures, one in six authors were limiting what they said or avoiding certain topics for fear of reprisals.[36] Such chilling effects are a serious matter when it comes to civil liberties and human



rights. They may not sound very tangible but they are all too real in their consequences.

Paralleling this, a Pew Internet and American Life study in 2014 showed that many in the US were withdrawing from using social media to discuss the Snowden findings. Only 42 per cent of those polled would risk such a discussion, compared with 86 per cent who would consider talking about mass surveillance offline. And even those social media users who might discuss Snowden with friends, face-to-face, were less likely than non-social media users to do so. This may reflect the fact that Facebook was one of the companies named within the post-Snowden debate, but nonetheless it at least suggests that social media are not necessarily a space where users feel freer than in offline relationships to discuss matters like this.[37]

What this shows, rather starkly, is that in the aftermath of the Snowden revelations, the choice of supposed security is very much at the expense of liberty. People are increasingly suspicious and wary. The spectre of fear is abroad, fostered by governments reacting hastily and ill-advisedly to attacks that may be described as 'terrorist' ones, and further amplified by mass media. This is deeply destructive of trust and care. How can cooperation, so vital to any democracy, develop when it is stretched to tearing point by uncertainty and distrust? If we are scared to speak or write about certain topics, democracy, dignity and political debate stand little chance.

## Democracy and Surveillance: Security Trumps Politics

Can mass surveillance ever be consistent with democracy? It is fair to say that surveillance and democracy have an unsettled and tense relationship. Surveillance can curb freedoms, inhibit democracy and, at worst, lead to totalitarianism – as

George Orwell and Hannah Arendt famously feared. For Arendt, a political theorist who shone a light on totalitarianism in the 1950s and 1960s, signs that the state was tightening its grip included naming 'objective opponents', who changed depending on the circumstances, and having secret policing agencies – a 'state within the state' – whose task was 'not to discover crimes, but to be on guard when the government decides to arrest a certain category of the population'.[38] Do these not ring bells as we confront the realities revealed by Snowden?

For those who work within surveillance agencies, however, recognizing this may be extremely difficult. Snowden himself speaks of the everyday routines that make operatives case-hardened within institutions like the NSA. Surveillance is what they do at their desks, manipulating the data on their computer screens. It is easy for them to lose sight of the life-altering and invasive ways that surveillance can impact people's prospects. Tens of thousands of employees work in these agencies in the US alone and the growth of intelligence services since 9/11 has been huge.[39] No wonder Arendt, speaking of a quite different context and time, noted that apparently humane citizens could, when they worked in their official bureaucratic capacity, unwittingly help the Holocaust to happen. She called it the 'banality of evil'.[40]

But what is democracy? Power exercised by people? Open procedures with equal rights to speak? Struggling to keep the public domain public?[41] Many would argue that democracy can contribute to effective decision-making and protect from corruptions of power.[42] Key aspects of democracy that have a bearing on surveillance include the accountability of government to its citizens. This means that citizens need access to information and a free press to assess government. Civil liberties and human rights protect these. The problem is that in the twenty-first century the world has moved on from



when Orwell and Arendt were its critics. The state is all too often a *corporate* state that pays lip-service to democratic ideals and simultaneously makes authentic participation very difficult.[43] And it has built a surveillance engine, as revealed by Snowden, that is having negative – and potentially devastating – effects on democracy.

As previously stated, surveillance is monitoring for intervention. Mushrooming surveillance alters the dynamics of visibility. Yet today, surveillance is normalized in the routines of everyday life, with worries only about its 'excesses'. Generally, the growth of surveillance seems to be seen more as necessary than negative. Few appear to see mass surveillance as a danger for democracy, eroding democratic institutions and public trust. It is true, of course, that in some respects democracy depends on surveillance. The same list of citizens that ensures 'one person one vote' may also be used to augment state power. Voter lists and registration may have positive effects in increasing development in contemporary as well as in historical societies.[44] Such ambiguities are ever-present and complicate simple stories of surveillance. But they never make surveillance neutral. They should not distract us from the stark realities of the apparently uncontrolled surveillance currently corroding the basic structural supports of democracy.

As well, equal citizenship may be eroded by categorical sorting, targeted voter systems and the like, each of which is surveillance-enabled. Even information narrowcasting on the internet, based on 'customized' contact, depends on personal data analysis. It creates what internet commentator Eli Pariser calls 'filter bubbles', in which people find their views reinforced through an echo-chamber of 'personalization' rather than engaging in broader debate.[45] This can produce less interest in the outlook and practices of others. One could be forgiven for thinking that such filter bubbles already play

a key role in distracting attention from looming issues like mass surveillance and creating a narrowly informed or passive citizenry.

Some worry, beyond this, that in post-Snowden times we may move away from both democracy and politics itself. Since 9/11 it has become clear that security trumps politics. A perceived crisis gave birth to emergency measures; exceptional circumstances demanded immediate, visible and appropriate action. The problem, as Italian philosopher Giorgio Agamben reminds us, is that while such 'states of exception' – where law is temporarily suspended for the public good – may be needed in the heat of the moment, they are meant to be short-lived, limited. But now classified 'reasons of state' make them permanent. Two things happen, or rather, do not happen: security remains ill-defined and no formal state of exception is declared.[46]

Firstly, security is paraded as a priority but what security actually entails remains cloudy. It seems amazing that the 'security' slogan that has dominated global politics as well as many realities of everyday life for more than a decade lacks clear definition. It is of course used in very different ways in different contexts. The idea that aiding the escape from poverty could be construed as a quest for security has been displaced by security as the control of terrorism in many countries of the global north but not, until recently, in the global south.[47]

As Lucia Zedner, professor of criminology, dramatically notes, security has the qualities of an errant fire truck. It is permitted to drive through city streets with lights flashing and sirens blaring even at risk of harming other road users. She wisely continues, 'The pursuit of security signals an urgency and importance that stifles debates as to priorities, resources and countervailing interests. To invoke security is to move to foreclose debate as to the wisdom of a policy or



the necessity of a measure.'[48] Security becomes of the utmost importance.

Thankfully, this is recognized in some important post-Snowden documents, such as the American *NSA Report*. The authors make it quite clear that security should be attached with equal strength to the words 'national' and 'personal'.[49] The latter includes, they say, Fourth Amendment rights to be 'secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…' They also reject outright the insidious view that a 'balance' must be sought between these two understandings of security. 'In a free society,' they assert, 'public officials should never engage in surveillance to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism or dissent; to help their preferred companies or industries…' and so on.[50] But will these words be heeded?

The frequency with which one hears of the 'balance' or 'trade-off' between privacy and security, or liberty and security, is matched only by its hollowness. Some legal experts love this. They hold 'threats' in one hand and 'individual harms' in the other, frequently forgetting that privacy is about relationships and the common good. 'Balance' really means nothing but it does lend spurious weight to the claim that rights to privacy, freedom of speech or whatever have to be curtailed in the quest for a greater good of a vague and undefined national security. Many have rejected the false splitting of 'national' and 'personal' concerns but as yet, alas, to no avail, at least in public attitudes.[51] Yet the only way to restore the public's frayed confidence in intelligence agencies and indeed in Western governments in general – as far as the shibboleth of security is concerned – is both to define terms clearly and to be transparent about how goals in each area are being sought.

Secondly, the lack of any formal declaration of a state of exception emerges from a steady but secretive process of changing the rules for dealing with crime. There is a marked shift from trying to understand *causes*, to managing *effects*. Crime control generally has shifted since the later twentieth century away from attempting to understand the environmental and social roots of certain types of crime and towards dealing with its impact.[52] This is why, for example, Prime Minister Stephen Harper of Canada cautions against 'committing sociology' when trying to understand the case of hundreds of missing and murdered Aboriginal women. Causes have to be known, effects call for control.

Agamben uses the example of biometrics, which were first used to check on previous offences and had no role in crime prevention. During the twentieth century, biometrics was increasingly applied to other areas of life, such that any and all citizens might be subject to biometric identification and authentication. Today this has expanded even further. We may use biometric controls to enter our offices or our cars, to cross borders, and even children may use them to purchase food in the school lunch break. Well beyond fingerprints, then, many biometric technologies have spread into numerous areas of everyday life, where a generalized control is evident – but often, no comment is made. It is taken for granted. Normal.

Modern dreams of citizenship seem rather detached from the passive citizenship of today. If Agamben is right in his fears about biometrics, it is not our place in the public sphere but our biological and now metadata that yields our 'identity'. Risk management approaches, dominant in the US and Europe since the 1980s, encourage officials to think that all citizens may be potential terrorists, and therefore control is clearly appropriate. Such modes of governance fit well with free market economics, because the right task of government



is seen as controlling effects, not querying causes. Hence the enhanced policing becomes more and more militarized and information-intensive. And if we are all potential terrorists then the close attention by authorities paid to dissidents, protesters and whistleblowers makes sense. The active and adversarial citizens assumed by classic democratic theory are unwelcome today. All citizens are being reclassified as potential threats to state security.

## Beyond Privacy?

The story of Faisal Gill demonstrates that much is at stake following the Snowden revelations. In particular, while privacy is tremendously valuable as a mobilizing slogan, it can easily be reduced to abstract matters with little connection to the real world. And it can be domesticated and used as a means of indicating that organizations are 'clean' – they can check the privacy boxes and continue their practices. Privacy, paradoxically, may enable surveillance. Alternatively, the kind of privacy that makes sense in post-Snowden times sees the common good as paramount, and cares deeply about protecting the other person, not merely about 'my privacy'.

Faisal Gill's story also shows how surveillance is a means of social sorting. In this case, the sorting negatively discriminates between different groups in the population so that one group can be treated differently from another. This example shows how easily a social category may be used to expand the range of a prejudicial conjunction of terms: 'Muslim' and 'security threat'. And it indicates how correct Snowden is to say that 'your rights matter because you never know when you may need them'. Faisal Gill imagined that, as a responsible citizen, he had nothing to hide or to fear. In fact, he was under constant surveillance simply because of his

identification as a Muslim. Privacy connects here with religious freedom.

Snowden also asks what kind of world we want to live in? Is it one marked by fear and mutual suspicion, where data is collected promiscuously and kept forever, in systems that never forget, making forgiveness obsolete and creating much to fear even though you have nothing to hide? Is it one where vulnerability is amplified, democracy diminished and where ordinary people are more exposed to organizations that are themselves more opaque? Or is it a different kind of society, the contours of which we can imagine but not yet experience?

The issue of 'framing' really applies to the whole question of surveillance in the twenty-first century. How do we think about these large and looming questions? How important is internet privacy – and indeed the role of the world's nation-states in monitoring and tracking individuals using metadata? Should we ignore such matters, assuming that privacy is a thing of the past? Or should we shrink into a paranoid state, refusing to participate in the online world, trashing our smartphones and retreating into a realm of disconnection and dystopian fears? Or is there another way to approach the world that Snowden's stolen documents have revealed?

# 5

# FRAMING FUTURES

Do we want to live in a controlled society or do we want to live in a free society? That's the fundamental question we're being faced with.

Edward Snowden, July 2014

On several occasions, Edward Snowden has observed that the world we have made is not merely 'Orwellian'. It is something much worse. And while his main focus is on the technological capacities that can easily turn an open internet into a cyber-cage, it is worth standing back to get a wider angle. Certainly, rampant mass surveillance is a deeply disturbing development and the NSA and its partners must become far more accountable and transparent if democratic rights are to be respected. But as we have seen, the internet as currently configured displays features that make it inherently surveillant, and this also goes for the whole 'networked society' and the global power flows that characterize it today. As Snowden