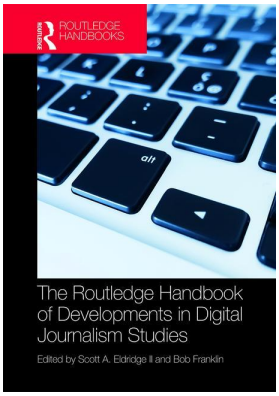

The Routledge Handbook of Developments in Digital Journalism Studies

Scott A. Eldridge, Bob Franklin

Journalistic Freedom and the Surveillance of Journalists Post-Snowden

Publication details
https://www.routledgehandbooks.com/doi/10.4324/9781315270449-28
Paul Lashmar
Published online on: 30 Aug 2018

27

JOURNALISTIC FREEDOM AND THE SURVEILLANCE OF JOURNALISTS POST-SNOWDEN

Paul Lashmar

A paradigmatic shift is sometimes revealed by an unanticipated and extraordinary event, and so it was with Edward Snowden in 2013. A National Security Agency (NSA) contractor, Snowden was so appalled at the exponential expansion of covert digital surveillance that he decided it was his moral duty to inform the public, indeed the world. This he did from a hotel room in Hong Kong when he gave a small group of selected journalists access to 1.7 million classified documents taken from the NSA. These documents revealed the global snooping capabilities of the NSA and its 'Five Eyes' intelligence agency partners (ASIO in Australia, CSE in Canada, GCSB in New Zealand, and the GCHQ in United Kingdom). The Five Eyes can vacuum up just about all digital communications anywhere, anytime, and much else besides if they are so minded. Many who take a deep interest in signals intelligence thought these Anglo-Saxon agencies had probably increased their capabilities since 9/11, but even they were shocked when Snowden revealed the sheer scale – it far exceeded any estimate of capability.

From Snowden's leaked documents, journalist Glenn Greenwald discovered the Five Eyes' mantra is "Collect it all". In one article he quotes from his favorite NSA document – a favorite because of its clarity in terms of just how comprehensive collection is:

> At the top of the document, it says "new collection posture". This is the NSA describing its new collection position, and right underneath is a really ugly, though helpful, circle with six points on it.
>
> *(Bell et al., 2017: 45)*

Greenwald goes on to detail how "Each of the six points has a different phrase that elaborates on the 'Collect It All' mandate", adding:

> So you go clockwise around the circle, and the top it says "Sniff It All" and then it says "Know It All," "Collect It All," "Process It All," "Exploit It All"; and then the last one is "Partner It All."
>
> *(ibid: 45)*

He continued:

> This then is the institutional mandate for the NSA – it is collecting billions and billions of telephone calls and emails every single day from populations and nations all over the world including our own.
>
> *(ibid: 45)*

Five years on from Snowden's revelations, there has now been time to assess the impact of Snowden's controversial leak. In the months immediately after he went public (September 2013 – February 2014), I interviewed journalists from across the Five Eyes countries for their assessment of Snowden and his revelations (Lashmar, 2016). I chose investigative journalists with national security reporting experience who are more likely to have a deep knowledge about what Snowden meant for the wider public and for journalism. They are also likely to be the journalists most 'at risk' from the surveillance capabilities of these agencies. As the general counselor for BuzzFeed, Nabiha Syed observed:

> There has always been some information asymmetry between reporters acting in the public interest and powerful organizations – like government agencies – that possess critical information. Increasingly, that imbalance is tilting against the interest of two critical groups: national security reporters and independent journalists.
>
> *(Bell et al., 2017: 142)*

My research cohort included reporters from both groups. In spring 2017 I went back to those I had originally interviewed and, where possible, interviewed them again. There had been some changes; one interviewee, Gavin McFadyen of the UK's Centre for Investigative Journalism, had died, a sad loss. Others had since moved away from national security reporting and felt they had nothing new to add. I approached roughly 20 journalists and was able to interview 12 between April and May 2017. There were at least two reporters from each of the Five Eyes countries. The journalists were; Andrew Fowler (formerly on Australia Broadcasting Corporation's *Four Corners* program) and Dylan Welch (ABC's 7.30 show) from Australia; Jim Bronskill (Canada Press), Andrew Mitrovica (freelance), and David Seglins (CBC) for Canada; David Fisher (*New Zealand Herald*) and Nick Hager (freelance and New Zealand's leading investigative reporter) for New Zealand; Duncan Campbell (intelligence expert and freelance journalist), Meirion Jones (ex-BBC and Bureau of Investigative Journalism), and Peter Taylor (BBC *Panorama*) in the UK; and Scott Shane (*New York Times*) and Jeff Richelson (National Security Archive) in the US. All have reported on intelligence agency excesses. At least three (Campbell, Hager, and Fowler) have been subject to security agency raids in their careers as a result of their stories. All have reported on or used the Snowden documents. One had met Snowden (Taylor), and others worked with the Greenwald team to some extent.

The semi-structured interviews I conducted with them form the basis of the research for this chapter. In addition, I conducted a review of books, reports, chapters, and papers on the impact of Snowden for journalists and their sources (see: Bell et al., 2017; Fowler, 2015; Kuehn, 2016; Bauman et al., 2014; Moore, 2014).

Perceptions of Snowden

In the immediate aftermath of Edward Snowden going public, the former NSA and CIA employee was applauded by some commentators as a hero, but others accused him of being a traitor and worse. The former director of the NSA, General Keith B. Alexander, stated that his leaks had resulted in "the greatest damage to our combined nations' intelligence systems that we have ever suffered" (MacAskill, 2014). British intelligence has spoken of areas of the world having "gone

dark" and of disruption caused to intelligence gathering. Back in 2013, some commentators and journalists posited that Snowden was working for Russian or Chinese intelligence. However, that criticism seems to have receded, and whether critics are for or against him, his sincerity is rarely now questioned. At the time of writing he remains in Russia and would face serious charges if he returned to the US. In 2015, Peter Taylor, one of the BBC's most experienced current affairs journalists, made a Panorama program about surveillance.

> I was fortunate enough to meet Edward Snowden in Moscow and spent about two hours with him. Before I met him, I was never quite sure about him. When I met him I was in no doubt about his sincerity, motivation, and fierce determination to out the things he thought the public should know. He had a powerful feeling the public was being kept in the dark.

Perhaps not surprisingly, as investigative journalists, all of the interviewees were in favor of what Snowden had done and felt that releasing information to the public was important. Some interviewees described Snowden as a hero (Mitrovica, Seglins). Andrew Mitrovica said, "We owe Snowden a debt of gratitude for risking his safety and freedom". Mitrovica said he was frustrated in the years before Snowden that the public and editors were not taking surveillance seriously. But Snowden's leaks changed that: "The public imagination got caught up in what he was doing. I thank him for trying to help make these things known to the public".

The name Snowden, it seems, has also become shorthand for global mass surveillance.

Impact of Snowden

Most of the interviewees felt that Snowden's revelations had reached a global audience and that, in terms of considering privacy and surveillance, there is a before and after Snowden. David Fisher said, "In the intelligence and the security space there is far greater awareness of surveillance issues and privacy issues". He believed that the public, at least in New Zealand, now has no expectation of privacy. Referring to the Five Eyes eavesdropping agencies, Fisher said: "Snowden has contextualized what we are dealing with now. The power they have, if they choose to use it, is awesome".

Asked about the impact his revelations had, the responses from those interviewed were varied. Peter Taylor felt that what Snowden had done was "hugely important". Mitrovica felt the releases had impacted hugely on the public and "made what was going on clear". Scott Shane said Snowden had raised awareness. The US interviewees reported a mixed reaction from the US public. Shane noted that in response to the Snowden revelations:

> About half of Americans and about half of Congress were unhappy with some of what was exposed, primarily the phone call metadata, and the Obama administration and Congress scaled things back and changed the procedure to increase privacy protection for Americans and made it less possible for the government to collect and store data on millions of Americans.

Shane emphasized that the NSA is so powerful that it needs to be closely monitored: "The capabilities of NSA obviously are so consequential that everybody needs to keep a close track".

Duncan Campbell, who is UK journalism's foremost independent expert on signals intelligence (SIGINT), was surprised by the scale of the surveillance capability revealed by the documents. The scholarly Jeff Richelson, who was one of the leading American independent experts on SIGINT, said the "vastness" of the Five Eyes operation did surprise him. He said the documents:

> dramatically shifted the understanding of the nature of Sigint by the US and the British in terms both of the reach of it but also in terms of targeting digital networks and extracting intelligence from digital networks, and the lengths they went to and had gone to, and presumably are going, to get that information in terms of not simply basic hacking or passive intercept but also implants or planting devices in computers they have diverted.

As to what the impact on the public had been, Richelson did not feel qualified to comment. The UK's Meirion Jones was the most skeptical of the interviewees concerning impact and felt the revelations merely confirmed what the public and journalists had suspected. Canada's Dave Seglins, who is an experienced CBC broadcaster on the national security beat, said he was "shocked at the initial stories", but he felt that Canadians were less skeptical than Americans of national authorities. Fellow Canadian Andrew Mitrovica felt Snowden had become a major cultural figure in the world. Jim Bronskill agreed that Snowden had reset the public debate: "It was useful and still is in the sense people are more mindful of the fact there are agencies collecting intelligence, and with modern tools it is infinitely easier to do, and it is happening".

Nicky Hager, who has had a number of run-ins with intelligence agencies in New Zealand over his investigations, stated that the Snowden revelations were "absolutely incredible" and felt "there had been a high level of public support for Snowden". He commented: "The New Zealand public at large had a much larger reaction to the overall world news than stories about New Zealand". David Fisher and Hager both said there was, initially, a big reaction in New Zealand, with town hall meetings and public demonstrations in the months after Snowden's leaks. Author of *The War on Journalism* (2015), Andrew Fowler, said the Australian reaction was divided. The public, he observed: "Have been, I would say quite supportive, in the sense that they have always believed their communications were being interfered with and their data might not be safe; but this provided absolute proof of it". Fowler and Dylan Welch felt that the Australian public did not react strongly, as they are very conservative in their views when it comes to intelligence issues. In the UK, Meirion Jones said the public reaction was mixed, but believes that if anything, the revelations resulted in sizeable part of the UK public having increased pride in the intelligence services: "That British intelligence is still something important, that they are ranked up there with the Americans, dirtier than the Americans, it appeals to a James Bond aura, for them it wasn't negative".

One of the most interesting aspects of the UK reaction is that in June 2013 much of the UK press, particularly the *Telegraph*, the *Sun*, and *The Daily Mail*, turned on the *Guardian* for printing Snowden documents and sided with the government and intelligence communities' condemnation. Campbell observed that coverage of Snowden in the UK was: "Highly slanted and quite significant in that the voice of Snowden was muted, so the message was really only conveyed by The *Guardian* and yes, the BBC, but muted through the onerous processes of purported balance".

In the other Five Eyes countries, there was much less of a tendency for the other news media to turn on the news organizations that had published exclusive Snowden material.

I asked interviewees how they would measure Snowden as a paradigmatic event – for instance, how they would compare it with Watergate, perhaps the most recognized news story where the news media had clashed with the secret state. Canada's Dave Seglins and Andrew Mitrovica both felt the Snowden affair was of global significance. Seglins stated:

> Snowden was more important than Watergate. Watergate pierced the veneer of moral leadership in the US but had less of an impact on the citizens of the world. I think the Snowden revelations instantly ripped the shroud of secrecy from activities of the Five Eyes countries but also made the entire world aware, realize what was technologically

> capable, possible. So I think it has far reaching consequences for people around the world and not just in the Five Eyes countries.

The collection obsession

Duncan Campbell was very concerned that Snowden coverage had been too focused on bulk collection and too little had been said about what GCHQ did with the data it collected. Campbell pointed out GCHQ has "customers": "It's a business, that's its *raison d-être*". He noted GCHQ has customer relations teams, a sales force, and delivery drivers – and for all the reporting of Snowden's UK documents highlighting GCHQ's role:

> It only focuses on one aspect – collection – the systems that steal all our data. It doesn't look at the intelligence process in the round, because for the most part that is what these documents see, and generally when they did, with some salient exceptions, that is not what the journalists went for. It seemed sexy to describe massive scoops on internet cables and the factors of scale, which is truly astonishing and so on. That criticism can probably be made of me.

He continued:

> The fact of the matter is, to understand in its context, the harm or good that may be done by signal intelligence agencies, you have to look at the tasking, the collection management, the analysis process, and above all the consumer reporting channel because the core interactions are not collection directed against the citizen, or the business or the target – they are the customer – who the government pays for – the customer gets spy data.

He then observed:

> Then the second interaction that matters is – what is done with it? So if the Snowden documents, which they do on some occasions, speak to all of those processes, they clearly have more force and show more of the picture, and when they don't, they certainly show collection capability and scale. But what is done with it?

Campbell made the point that it is important to understand who gets the raw intelligence from GCHQ surveillance – whether it is the Defence Intelligence (DI), MI6, MI5, or the police – and what they do with it and whether it infringes the target's rights under Article 8. This is a point that is equally relevant to other Five Eyes countries. Indeed, the intelligence lobby was frustrated by this post-Snowden emphasis on collection, which they describe as bulk collection, and argue that is not the same as mass surveillance, as they filter out most data to focus on targets. These are indeed set by their customers and do not eavesdrop on the public at large. However, we have little idea how collected data impacts on the civil liberties of 'targets'.

Impact on journalists

As UNESCO researchers noted:

> While the rapidly emerging digital environment offers great opportunities for journalists to investigate and report information in the public interest, it also poses particular challenges regarding the privacy and safety of journalistic sources
>
> *(UNESCO, 2017: 5)*

The Snowden documents revealed that some journalists were the targets of intelligence agencies. In 2013, *Der Spiegel* reported that the NSA had intercepted, read, and analyzed internal communications at Al Jazeera that had been encrypted by the news organization (*Der Spiegel,* 2013). There are many other examples. In early 2015, the *Guardian* published a Snowden document that revealed that a GCHQ information security assessment listed "investigative journalists" in a threat hierarchy (Ball, 2015). Such incursions on journalists' digital communications compromise the globally established ethical obligation upon journalists to avoid revealing the identity of their confidential sources.

> The issue of source protection has come to intersect with the issues of mass surveillance, targeted surveillance, data retention, the spill-over effects of antiterrorism/national security legislation, and the role of third party Internet companies known as "intermediaries".
>
> *(UNESCO, 2017: 18)*

The Pew Center's research in the United States found that 64% of investigative journalists surveyed believed that the U.S. government collected data about their communications. The figure rose to 71% among national political reporters and those who report foreign affairs and national security issues. Ninety percent of U.S. investigative journalists who responded to the Pew survey believed that their ISP would routinely share their data with the NSA, while more than 70% reported that they had little confidence in ISPs' ability to protect their data (UNESCO, 2017: 103). Nearly all my interviewees felt that Snowden's revelations had a big impact on journalists generally and had raised very serious questions about whether journalists could protect their sources. Shane said: "There was more awareness amongst journalists". Back in 2014, Duncan Campbell counseled it was important to keep things in perspective, and only a relatively small number of journalists are likely to be subject to surveillance by the NSA network: "The impact of Snowden's revelations should not really be overstated for journalism, because the most critical aspect relates to the conduct of the intelligence" (quoted in Lashmar, 2016).

In 2016, Campbell maintained this position. New Zealand's David Fisher observed much the same for most investigations but stated it is a different story if you are investigating Five Eyes agencies: "If you are fucking with them there is no way they are not going to find out". Otherwise sensible trade craft will do, he said:

> If it's the spies you are messing with – they are going to track every single bit of metadata you've got. They are going to intercept every bit of commination you've got. When you are out of house, they will break in and download everything on your computers.

Fisher thought that sources are more alert: "There has been a chilling effect". Meirion Jones and Taylor said the Snowden revelations had impacted on sources. Shane reported it had an impact on sources, but this had been somewhat negated by Trump, where sources are queuing up to dish the dirt on the White House. Fowler was concerned how cavalier some sources are and that he still gets emails that could incriminate the sender. Mitrovica was bullish: "It's not had a chilling effect on me" – nor was he worried about the impact on sources – "I think some sources have been emboldened by Snowden".

Methods

When it came to protecting their sources, the interviewees' reaction to changing procedures was mixed. Some (Fowler, Welch, Seglins, Fisher, Shane) said they had tightened up their security since Snowden to protect their sources. Shane said he had become more cautious but made

the point that in the US it was not just Snowden's revelations that influenced journalists but the Obama administration's prosecution of journalist sources that had impacted on journalists. Indeed, one of Shane's own contacts, John Kiriakou, had been prosecuted and jailed. David Seglins said that working with and reading the Snowden documents had fundamentally changed his understanding of operational security as a journalist:

> Everything from storage of documents to the use of encryption, encrypted communication, encrypted data storage, to how our mobile devices are potential listening devices and how that affects a journalist's ability to travel to places, meet sources, have discussions with absolute certainty we are not being recorded or monitored or tracked.

Hager and Jones said that they had always employed rigorous source protections methods, so had no plan to change. "I would rather lose a story than a source", said Jones. Some interviewees have incorporated new counter-surveillance digital methods routinely into their work. Encryption has become a regular tool in a way it was not before Snowden. Shane said he uses encrypted email. Some are using PGP technology (Fowler, Welch, Hager, Seglins, Fisher, Jones, Shane) as necessary, and some use TOR for browsing (Seglins, Jones, Hager). Like Shane, some also use encrypted phone apps:

> One of the things that has changed since we last talked is the proliferation of encryption communication apps. Many of us have run through the various ones, Silent Circle, WhatsApp, Signal, so there is an increasing availability of encrypted communications. I'm certainly more aware of what I am putting into a storable electronic record.

Some interviewees now include the PGP key and other encryption contact information into their email or social media addresses. Welch said this told potential sources that he is serious about source protection:

> I list it all. I tell people where they can find my PGP, my public key. I tell them I have every single one of the encrypted apps on my phone. I use them a lot. I don't try to hide it.

Some reported their news organizations had decided to set up Secure Drop (a secure and encrypted inbox) facilities for potential sources to send material to (this includes *Sydney Morning Herald*, Canadian Broadcasting Corporation, *New York Times*, the Bureau for Investigative Journalism). Other organizations have decided against it (ABC in Australia, *New Zealand Herald*, and Canada News). Fisher pointed out that using encryption can be a 'red flag' to interested intelligence agencies that you are communicating with someone they might be interested in. Most journalists who use encryption said it was only a partial solution to be used with care. There was clear concern that the Five Eyes may have found ways to break encryption. Taylor said that while examining the Snowden documents:

> One thing that really surprised me, and really it should not have done, was that he had GCHQ material from a training manual. The intelligence service GCHQ could tap into your phone by planting malware inside it and listen to your conversations and take photos of you and whoever you were with, even though your phone appeared to be off. That really shook me.

Scott Shane said the *New York Times* made a lot of effort to protect sources and had recently appointed a newsroom security adviser, and journalists were given training and advice from

lawyers. Almost all interviewees emphasized the importance of 'non-digital' means of communication with sources, making sure there was no digital footprint of the meeting – leaving mobile phones and laptops at home. Jones said it was important to tell sources that you cannot guarantee to protect them, though you would do your best.

Damage to national security

When the Snowden material was published, politicians and intelligence chiefs attacked journalists for publishing the classified documents, and it was not uncommon for these critics to accuse editors of putting lives in danger and damaging the ability of national security agencies to monitor and deter terrorists. Interviewees were varied in their responses about whether Snowden had damaged national security. Campbell thought there might have been an impact on operational effectiveness. Richelson thought some techniques might have been revealed. After British intelligence claimed to him that Snowden had put lives in danger, Taylor asked them to identify an example. They failed to do so, saying: "We can't comment on such information". He does feel that there was some general damage, but Snowden also performed a public service. Often robust in his position, Fisher in New Zealand took the view that claims of damage were "a load of bollocks", adding: "If there had been any real consequences of that occurring that would have been rammed down all our throats". Fowler in Australia did not believe there had been any damage. Neither did Mitrovica in Canada: "No it's a myth, it hasn't damaged their effectiveness. They always trot this out all the time".

Seglins noted that if Canadians were to have confidence in their national security:

> Part of national security is confidence in democracy, confidence in judicial oversight, confidence in our law enforcement and intelligence agencies. And if they were operating in the dark, and/or illegally, and/or counter to public trust, then I would say the Snowden leaks have enhanced national security because we were growing for a long time in the dark, not knowing what our law enforcement agencies were up to. And that secrecy and that vacuum of public knowledge and oversight are where corruptions and breakdowns occur, we know that.

Shane said there may have been some damage to specific operations, but that was the price of democratic debate:

> If you live inside those bureaucracies you begin to think that it's the end of the world when someone learns something about what you are up to. But these trade-offs exist in any democracy. We would all be safer from terrorism if there was not restrictions on these agencies and they recorded and stored all America's conversations and emails on a permanent basis. We would all be safe from terrorism. On the other hand, that's not the way we want to live, and I think these agencies sometimes forget that.

Another major complaint from politicians and intelligence chiefs is that due to Snowden's revelations, not only are journalists, sources, and the public much more likely to use encryption but so are criminals and terrorists. Agencies complain that some of their key targets "have gone dark" because of encryption. Taylor made the point: "Remember Snowden was in early days of encryption. Encryption is now the big problem". Indeed, Snowden has publicly supported people using encryption.

It is worth noting none of those interviewed disputed that there is a role for intelligence agencies in tackling terrorism. Duncan Campbell took the view that "from available evidence", British intelligence was doing a good job.

Responsibility of the media

At the time of writing, 6,000 Snowden documents have been released into the public domain through a set of rigid procedures by a team of journalists led by Glenn Greenwald and Laura Poitras. No interviewee thought the media that dealt with the Snowden material had acted irresponsibly. Taylor thought the *Guardian*, as the first news organization to publish Snowden documents, had been professional. Those who had used documents had checked with formal intelligence links to make sure that they were not going to do any inadvertent damage. In some cases extensive and repeated checks were made, and occasionally certain aspects of stories were dropped if the news organization thought the national security people had made a compelling case. Rusbridger has said the *Guardian* had over 100 contacts with the authorities before publication (Ponsford, 2014). Shane, Taylor, and Seglins reported detailed conversations. Redaction was also used. Journalists (Taylor, Shane, Seglins) who dealt with these negotiations were critical of the initial position of intelligence chiefs, which was to say nothing should be published. Over a period of time, the negotiations became more sensible, and the intelligence agencies realized that the journalists were more likely to listen if they made a good case for an element not being published. Hager was more skeptical about any opening up:

> There wasn't a discussion. The most frustrating thing about intelligence as a public policy issue, or as part of the life of the country, which it plainly is, is that there is a sense of entitlement on the side of the authorities not to engage in debate, and they know perfectly well that while that has an operational element it is also highly convenient.

Hager did not confer with the intelligence agencies about the content of his Snowden documents because, he says, the agencies were incapable of a sensible discussion. Instead he went to "a lot of trouble to make sure we did not tell stories that would really harm something that really matters". Hager said there were aspects of New Zealand's surveillance operations in Bangladesh "that were really dodgy" and, if revealed, could have "brought a dangerous backlash to New Zealand", so he withheld the details.

Taylor said that despite the hard line initially taken by the intelligence chiefs that the BBC should not broadcast Snowden documents, that after the Panorama program went out they seemed to think it was fair. Fowler stated he did not think that journalists should refer back to the agencies:

> I do think they acted responsibly. In fact, my argument is that I think the journalists acted, what I would call, without being too cute, too responsibly. I would trust the judgment of a journalist whether or not to publish the material rather than running it past government, as seems to have been case with the Snowden documents. . . . I don't think a journalist should need to do that, make a call on that and live with that.

Laws

With the exception of the United States, interviewees in the other Five Eyes countries said new laws have been passed to enhance the power and scope of the intelligence agencies. In some cases the laws were on their way already at the time of Snowden releasing the documents, and in other cases the Snowden affair was either part or all of the reason for new laws. Nearly all the interviewees felt that the laws gave excessive power to the national security community. In some cases they took the view the laws were draconian. In the UK as a result of the Snowden revelations, in

February 2015, the intelligence watchdog, the Investigatory Powers Tribunal (IPT), found GCHQ had breached human rights conventions in relation to the UK's access to the NSA's bulk data collection program. Nonetheless the Investigatory Powers Act (a tougher and revised successor to the controversial 'Snooper's Charter') passed into law in 2016. As the act became law, Snowden tweeted: "The UK has just legalized the most extreme surveillance in the history of western democracy" (Snowden, 2016). The IPA is just one example of national security bodies being given more powers. In July 2014, the UK government fast-tracked a new Data Retention and Investigatory Powers Act as 'emergency legislation' and rushed it through parliament in a single day. The act was designed to revise UK data retention law in response to an April 2014 ruling by the European Court of Justice (ECJ) invalidating the 2009 Data Retention Directive. The law not only provides for ongoing blanket retention of communications data of UK residents, in direct contradiction with the ECJ ruling, it also extends the reach of UK interception powers by enabling the government to require companies based outside of the United Kingdom to comply with the UK's warrants. In addition, the UK's Law Commission has carried out for the government a consultation to update the Official Secrets Act into an Espionage Act. Critics say the initial proposals suggest that journalists, sources, and whistle-blowers will be vulnerable to imprisonment.

Some interviewees felt the Snowden leaks had given governments the justification to toughen the laws. In the UK, Taylor said: "The difference that Snowden has made is that we now have legislation that is far more embracing than its predecessor". David Fisher said that new legislation was proposed in New Zealand in 2014 and there were protests, but when a more "enhanced" legislation was passed in 2017, there were no protests. For Australia, Fowler said: "The government has introduced tough new laws as a result of Snowden, citing Snowden as one of the reasons why they had introduced them". As critics have noted, the initial draft of Australia's metadata legislation arrived without a dataset or safeguards. A review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) added 39 recommendations, including a request for a separate review on the impacts on journalists, the inclusion of a dataset, and additional oversight provisions. A mandatory two-year metadata-retention scheme was among the many anti-terrorism measures. In both Australia and the UK there have been examples of police using existing legislation, the Regulation of Investigatory Powers Act (RIPA) in the UK and the Telecommunications (Interception and Access) Act 1979 in Australia, in secret to identify sources by accessing journalists' metadata.

Andrew Mitrovica said the Canadian government had enacted "draconian pieces of anti-terrorism legalization" including anti-terrorism law C51 – "C51 broadens state powers to surveil individuals and broadens what is considered dissent". He added: "It's not surprising; governments inevitably act this way". Seglins said that the Trudeau government has conducted a review of legislation, and it is likely that it will include enhanced judicial oversight of the Canadian intelligence agencies. Despite all the new legislation, there has been little improvement for journalists and their sources. In 2016 in Canada, the courts have ordered a Vice reporter to hand over documents or face jail. Vice journalist Ben Makuch has been fighting a police order to hand over his correspondence with Farah Mohamed Shirdon – a man who left Calgary to allegedly fight with ISIS. Makuch refuses and was still in the court process at the time of writing.

The USA Freedom Act, which was passed by the House of Representatives in May 2015, reduces government bulk collection of U.S. phone records. Americans' phone records will still be hoovered up – but now by the telephone companies, not the NSA – and access to them will require a warranting process. Elements of transparency around government surveillance and the operations of the secret FISA court will be introduced.

Some interviewees noted that these laws made little or no provision for journalists undertaking their fourth estate role. The UNESCO report noted that, across 121 countries, technological developments and a change in operational methods of police and intelligence services are

redefining the legal classification of privacy and journalistic privilege internationally. The report also notes that alongside digital developments, in less than a decade, increasingly restrictive anti-terrorism and national security legislation has been passed into law that has or will override the existing legal protections, including those known as 'shield laws':

> This arises from moves to broaden the scope of "classified" information and exceptions to coverage, and to criminalize all disclosure of "secret" information (including in some cases, the publication thereof) irrespective of public interest or whistle-blowing considerations.
> *(2017: 20)*

UNESCO adds:

> The result of the increasing risk to both journalists and their sources is a further constraining, or "chilling", of public interest journalism dependent upon confidential sources.
> *(ibid: 20)*

Raising an ontological dilemma, Nicky Hager observed that knowledge of global surveillance may well have a profound effect on citizens' behavior and that journalists publicizing the issues might well not help. Hager felt that journalists have to report on intelligence and its excesses, but he also worried about being part of the chilling effect:

> I know, on the one hand, that unless we publicize and debate and kind of have real information rather than just vague fears, there can be no real progress. But on the other hand, to publicize is to add to this chilling effect, and I worry about that. I think it is a really important issue.

In Australia Fowler thought Snowden's revelations had a definite chilling effect on people's behavior: "If it has changed my behavior, it will have certainly changed the behavior of people I would normally talk to".

Conclusions

As Taylor, Hager, and others pointed out, this discussion over the surveillance state had largely closed down after 9/11. Twelve years later, Snowden revealed that we had sleepwalked into a world where total digital surveillance was not only possible but was happening. What the interviewees just about all agreed about was that Snowden had reset the public discussion for better or worse. Taylor thought Snowden's act in 2013 was "hugely important", adding, "It was of its time because secrecy had always been an issue, but at that particular time it had reached a head, and that again is one of the reasons why Snowden revealed it. He was genuinely shocked".

Interviewees felt that the changes in intelligence agencies' powers and capabilities were so great they needed to be referred back to the public, even if only for affirmation. Questions remain concerning whether the techno-optimistic focus of SIGINT agencies to ever expand the technology and 'collect it all' is the best means of deterring terrorism. In the UK and Europe, terrorism plots have been prevented, but there is a rise in the number of successful 'home grown' attacks.

The post-Snowden world is a troubling place for investigative journalists, whistle-blowers, and sources. It is clear that all five governments, whatever they said in public, had little respect for journalists' fourth estate role and were unmoved that the national security agenda had a by-product of making the job of journalists even harder. As the UNESCO report noted, the problem has grown in many countries, with tougher anti-terrorism laws that allow for access to

journalists' records and enforce assistance. State secrets acts are increasingly broadly defined and criminalize journalists who publish leaked information. This "occurs where it is un-checked by measures designed to preserve fundamental rights to freedom of expression and privacy". UNESCO adds: "In practice, this leads to what can be identified as a 'trumping effect', where national security and antiterrorism legislation effectively take precedence over legal and normative protections for confidential journalistic sources" (2017: 19).

From 2013 onwards in the United States, there was at least a discussion about the tensions between surveillance, privacy, and freedom of expression. By comparison, the UK government, intelligence chiefs, and even some editors took the approach to those who were concerned about Snowden's revelations: 'Move along please, there is nothing to see'. It was a monumental arrogance to decide that the public and journalists should not have the right to discuss such a major political change as the development of an infrastructure capable of total surveillance. Dressing it up as a necessary response to terrorism is just not good enough. Far from there being 'nothing to see', we have moved into a different type of society. The intelligence lobby are playing a 'dead bat' to the critical audience, while behind the scenes they lobby hard for further powers, resources, and capabilities.

That the government and intelligence lobby do not even want to debate compelling concerns that we have moved into a digital surveillance state is not evidence of a strong democratic government at work but, to the contrary, a victory for terrorism. To have so fundamentally changed the nature of UK society, to have made it so fearful, is a win for the terrorist and a defeat for a democratic nation. That governments have become more authoritarian is also demonstrated by the failure to make provision for journalists doing their fourth estate job, supposedly a vital independent oversight mechanism in a democracy. There is a clear drive to close down journalistic public interest endeavors for investigating malfeasance by the state, and especially when it comes to the excesses of the secret state. This is not just an issue for the Five Eyes countries but sets the tone for other countries, many of which are following suit, as the UNESCO report clearly shows. We can blame Snowden, but he did not set up the Five Eyes – he was the messenger, not the architect.

Journalists face an existential crisis. In the past, they could offer confidential sources a reasonable promise of anonymity provided that sensible precautions were taken. Now journalists have no precise idea of the level of risk their sources will face. Duncan Campbell makes the proportionality point that it is unlikely that journalists or their sources will be under digital surveillance unless they are delving into very sensitive areas like national security. The fact remains that journalists do not know if they are subject to surveillance.

Campbell is also correct that whether you call it bulk collection or mass surveillance, we are currently too focused on the sheer scale of surveillance, but we know nothing about those who are being targeted and the impact on their civil rights. In each of the Five Eyes, there have been recent examples of security services exceeding their remit. Perhaps the most telling comment in all the interviews and one that demonstrates the new paradigm came from Nicky Hager. He is profoundly concerned over the impact global surveillance may have on the citizen's behavior, and because of this "they grow differently as a person because they have a background sense of the lack of privacy". Privacy is a fundamental human condition, and we do not know yet the existential consequences of undermining the public's fundamental sense of privacy. This can be laid not only at the feet of Five Eyes but also of the internet giants like Google and Facebook, but the national security involvement brings a totalitarian element to the debate. If intelligence and surveillance are impacting negatively on ordinary people's lives, then we need to stop and debate this, not as the UK government and other Five Eyes' governments have done, ignoring dissent. What follows from ignoring dissent is the suppression of dissenters, and the tools for repression are now firmly in place to do exactly that.

Further reading

The writing of this chapter coincided with the publication of two excellent companion publications, Bell et al.'s *Journalism after Snowden* (2017) and UNESCO's *Protecting Journalism Sources in the Digital Age* (2017). I would also recommend Townend and Danbury's *Protecting Sources and Whistleblowers in the Digital Age*, an Information Law and Policy Centre report in association with Guardian News and Media. The issues in this chapter will be developed in my forthcoming book: *Spin, Spies and the Fourth Estate: British Intelligence and the Media.* Edinburgh University Press.

Acknowledgment

Jeff Richelson, one of the finest historians of U.S. intelligence, died in November 2017. This chapter is dedicated to him.

References

Ball, J. (2015, January 19) "GCHQ captured emails of journalists from top international media." *The Guardian*. Retrieved from www.theguardian.com/uknews/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-lemonde-reuters-nbc-washington-post (accessed 20 February).

Bauman, Z. et al. (2014) "After Snowden: Rethinking the impact of surveillance." *International Political Sociology*, 8(2), 121–140.

Bell, E., Owen, T., Korana, S. and Henrichsen, J. (2017) *Journalism After Snowden: The Future of the Free Press in the Surveillance State.* New York, NY: Columbia University Press.

Der Spiegel. (2013, August 31) *Snowden Document: NSA Spied on Al Jazeera Communications*. Retrieved from www.spiegel.de/international/world/nsa-spiedon-al-jazeera-communications-snowden-document-a-919681.html (accessed 26 May 2017).

Fisher, D. (2014, December 10) "Why NZ spy chiefs can no longer get away with saying 'we can neither confirm nor deny'." *New Zealand Herald*. Retrieved from www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11371394 (accessed 29 June 2017).

Fowler, A. (2015) *The War on Journalism*. Sydney: William Heinemann.

Kuehn, K. M. (2016) *The Post-Snowden Era: Mass Surveillance and Privacy in New Zealand*. Wellington: BWB Texts.

Lashmar, P. (2016) "No more sources? The impact of Snowden's revelations on journalists and their confidential sources." *Journalism Practice*, 11(6), 665–688.

MacAskill, E. (2014, June 24) "New NSA chief says 'sky not falling down' after Snowden revelations." *The Guardian*.

Moore, M. (2014) "RIP RIPA? Snowden, surveillance, and the inadequacies of our existing legal framework." *The Political Quarterly*, 85(2), 125–113.

Ponsford, D. (2014) "Rusbridger on how no journalist's sources are safe, joining IPSO and why he would have kept News of the World open." *Press Gazette*.

Snowden, E. (2016, November 17) "The UK has just legalized the most extreme surveillance in the history of western democracy." *Twitter Feed*. Retrieved from https://twitter.com/i/web/status/799371508808302596 (accessed 29 June 2017).

Townend, J. and Danbury, R. (2017) *Protecting Sources and Whistleblowers in the Digital Age*. doi: 10.2139/ssrn.2961911

UNESCO. (2017) "Protecting journalism sources in the digital age." *UNESCO Series on Internet Freedom*. Retrieved from http://en.unesco.org/news/unesco-releases-new-publication-protecting-journalism-sources-digital-age (accessed 25 May 2017).