SCOTTISH CHILLING

IMPACT OF GOVERNMENT AND CORPORATE SURVEILLANCE ON WRITERS

November 2018

Research conducted by Nik Williams (Scottish PEN), David McMenemy and Dr. Lauren Smith (Department of Computer and Information Sciences, University of Strathclyde)

Scottish PEN

defending the freedom of writers and readers

University of Strathclyde Glasgow
Scottish PEN is the Scottish Centre of PEN International and was founded in 1927 as a not-for-profit organisation that champions freedom of speech and literature across borders. Scottish PEN campaigns on behalf of the rights of writers both at home and abroad, ensuring they can express themselves fully free from the threats of violence, censorship, intimidation and interference. We have been vocal opponents to the silencing of writers across the world and have campaigned on behalf of writers including Raif Badawi, Anna Politkovskaya, Liu Xiaobo, Ragip Zarakolu and Lydia Cacho, as well as leading campaigns in Scotland to reform defamation law, oppose surveillance and champion Scottish writing in all its languages.

Scottish PEN is a registered Scottish Charity with the charity number SC008772. Scottish PEN is a SCIO (Scottish Charitable Incorporated Organisation).

Authors

David McMenemy

David McMenemy is a Lecturer in Information Science at the University of Strathclyde, and Deputy Director for Postgraduate Teaching. His research interests encompass issues around information law and ethics, including intellectual freedom, and freedom of expression, freedom of access to information, privacy, and the philosophy of information. He has also extensively researched around public library policy and development in the UK. He is author of The Public Library (Facet, 2009) and was Editor of Library Review between 2006-2011 as well as co-author of Librarianship: an introduction (2008), and A Handbook of Ethical Practice (2007).

Dr. Lauren Smith

Dr. Lauren Smith is a researcher-librarian interested in issues around information, agency and equity. She received a PhD from the Department of Computer and Information Sciences at the University of Strathclyde in 2016, following which she was a Research Associate in Information Sciences and Education at the university. Her research interests centre around social justice issues in librarianship, including information agency for political and civic engagement.

Nik Williams

Nik Williams is the project manager at Scottish PEN. He has led work on defamation reform, digital human rights and opposing surveillance reform in the UK, which includes leading security and privacy workshops around Scotland for libraries, schools and other groups. Nik has been published by openDemocracy, The Herald, The National, CommonSpace and Index on Censorship, as well as speaking on BBC Radio Scotland and RightsCon in Brussels in 2017.
1. INTRODUCTION

Nothing to hide, nothing to fear?

The Internet continues to redefine our relationship with the data we create and share. Every action we take online - whether browsing the web, communicating with friends, colleagues or family, navigating in a strange city or buying things online - generates data that can, if others are looking, reveal a great deal about our beliefs, routines, personalities and ideas – the Snowden revelations of 2013 revealed that in fact there are a large number of people paying attention.

Surveillance requires raw data to identify patterns and establish routines that can help the watcher derive meaning and plot potential next steps. According to IBM, ‘every day, we create 2.5 quintillion bytes of data’; this is the equivalent of 250,000 Libraries of Congress. This constant generation of raw data has afforded surveillance an unprecedented level of intimacy and access to our lives. It is this insight that can be leveraged to map our consumer habits and preferences, reveal membership of organisations or specific political beliefs or, in fact, reveal our guilt or innocence.

According to IBM, ‘every day, we create 2.5 quintillion bytes of data’; this is the equivalent of 250,000 Libraries of Congress

The NSA leaks shared to the world by whistle blower, Edward Snowden in 2013 brought to light the far reaching, near total powers of intelligence agencies to capture, retain, analyse and share online data generated by civilian populations across the globe, most notably in the ‘five eyes’ countries: UK, USA, Canada, Australia and New Zealand. The indiscriminate nature of such bulk powers is not limited to those suspected of any crime, settling instead to capture data on the population at large without their consent or knowledge. This redrew the understood reach and capabilities of states’ surveillance programmes and revealed the lack of public knowledge, consent or approval of such powers, even when faced with evolving and challenging security concerns.

Public perception of surveillance is hard to codify. In a 2014 poll, BBC found that 61% of those polled in the UK felt they were free from government surveillance irrespective of the powers that had been revealed by the NSA leaks the year before. When it comes to how perception is anchored on issues that are subject to increased media and political attention, the results reveal a level of ignorance in the wider population. As the Investigatory Powers Act, which consolidates and modernises UK surveillance legislation, was being debated in the Houses of Parliament, Liberty commissioned a ComRes poll and found that “nearly three quarters (72%) [did not] know anything about [the] Investigatory Powers Bill – or have never even heard of it”.

The Snowden revelations revealed the space for advanced digital surveillance within functioning democracies was extensive. While this formed the basis of a debate on transparency, digital privacy and surveillance across the globe, in the UK, what Snowden revealed resulted in substantial reform of surveillance.

laws to bring what was revealed within a legislative framework. What followed was the Investigatory Powers Act that passed through the House of Commons in 2016. This legislation sought to modernise, consolidate and expand digital surveillance powers available to intelligence agencies, the police and public bodies across the country. Powers within this bill include the storage of web browsing history and app usage data (Internet connection records) of every British citizen held for 12 months by telecommunication providers to be accessed by over 40 public bodies; the ability for intelligence agencies to hack devices, networks and servers to bypass encryption, turn on webcams and microphones, access data, monitor Internet usage in real time, destroy the device, or use the device to hack others; to store, acquire and analyse data in bulk and establish obligations for telecommunications providers to undermine encryption or build in backdoors to their systems to support the government’s data collection aims. This expansion was framed with a quasi-legal, quasi-political oversight mechanism that establishes a requirement for a judicial commissioner to approve the decision of the Secretary of State.

Questions remain as to how data collection and retention on this scale are compatible with existing human rights protections. The Court of Justice of the European Union stated in relation to the Data Retention and Investigatory Powers Act that “legislation prescribing a general and indiscriminate retention of data...exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society”. Further to this, a 2018 ruling by the European Court of Human Rights found that the UK’s methods for bulk interception of online communications violated the right to privacy, as well as the right to free expression due to the lack of safeguards in relation to confidential journalistic materials. These rulings and the incorporation of a similar bulk powers regime in the Investigatory Powers Act raises significant challenges as to how surveillance powers can be lawfully deployed across the UK, in line with all human rights protections.

But beyond the deployment of this audacious piece of legislation, the continued evolution of digital surveillance (both state and corporate) in our society has demonstrated a significant shift in how we understand the seen and unseen transmission of data shared across the Internet, define ownership of personal data held by 3rd parties and establish robust human rights protections that remain relevant in the digital age. The right to privacy and the challenges that exist in the age of big data to enable us to fully realise this right has monopolised coverage of both the Snowden revelations and the passage of the Investigatory Powers Act. But the relationship between surveillance and free expression warrants further analysis and debate related to how the existence of imperceptible but ever-present surveillance changes the willingness of writers to express themselves, or in the words of Raymond Wacks, whether the “knowledge that our activities are, or even may be, monitored undermines our psychological and emotional autonomy”. If privacy is a foundational right, making it possible for us to fully realise and enjoy other rights – for example, the space within which to express ourselves or follow any religion of our choice free from the threat of violence, coercion or judgement – surveillance is not a question limited to privacy alone, it is something that

---

affects, modifies and recontextualises a wide range of our human rights and reshapes the complex interplay between the state, private service providers and the wider population across the globe. A YouGov poll in 2015 asked whether those polled believed that if GCHQ had the resources and capability to intercept/collect the Internet-based communications of each British citizen, would they trust them not to abuse that capability and more than half responded that they did not. This issue of trust is not limited to UK government agencies. A 2017 POLITICO/Morning Consult poll found that “half of the poll respondents said they do not trust broadband companies to keep their personal information private, 61 per cent and 59 per cent said they don’t trust Facebook and Twitter in the matter, respectively. Fifty-three per cent said they do not trust Google to keep their data private.”

The Censor in the Digital Age

The concept of ‘chilling’ is based on the concept that laws, actions or activities, from both state and non-state actors, can modify the actions of others, in this case the willingness to express themselves. This is not a phenomenon limited to that of speech, “the term is now used broadly to describe where human behaviours are effected or restricted as a result of laws or procedures that encourage individuals to limit behaviours that were previously seen as matter of fact.” The relationship between this form of chilling and surveillance is also not new. In 1972, the US Supreme Court, ruling on the Laird v. Tatum case, stated in regards to the impact of surveillance: “allegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm”. This tension highlights a central challenge when looking at self-censorship.

The forces that discourage expression are difficult to define by shape and size. When forces coalesce to discourage expression, we see different forms of censorship at play; explicit interference through the threat or application of violence, the creation of bureaucratic mechanisms by which certain groups are continually rendered void, alongside exorbitant registration fees or regulatory frameworks that establish overly restrictive membership criteria, among other methods by which expression is monitored, controlled and ultimately repressed. Self-censorship, or the mechanism by which individuals internalise restrictions and shape their creative output to adhere to the majority viewpoint is far harder to measure. Outright censorship as outlined above leaves a visible mark on the cultural landscape that can be measured; number of writers attacked, disappeared or threatened; costs of acquiring the necessary permit or registration; and the membership criteria of regulatory bodies are just a few of these markers. Self-censorship is far harder to track; how can you measure an absence of something that never existed because the author decided against committing it to a medium and making it available to others?

To give shape to our understanding of self-censorship, it is necessary to explore what forces may compel silence. These drivers to self-censorship overlap a great deal with acts of overt censorship. For example, if you

---

are a writer who has seen members of your writing community arrested or attacked you have witnessed acts of overt censorship, but upon seeing this, are you as willing to continue writing? By internalising the force exerted on others you are carrying out the function of censor towards your own output. But beyond these forces, others come to the fore when we seek to identify drivers to self-censorship. A key driver that has grown in significance and is at the centre of this report is how the perception of digital surveillance impacts writers’ willingness to express themselves. While surveillance does not exert the same direct pressure as overt censorship - it can however be used as a mechanism by which to implement these measures i.e. monitoring content that may violate laws such as criminal defamation or hate speech, or mapping relationships between actors to identify networks of interest – the impact of surveillance on self-censorship should not be ignored, especially when viewed in the context of progressive and multi-party democracies such as the UK. It is important to also consider, in relation to the coercive impact of surveillance, the notion of the panopticon, a widely used metaphor adapted from the prison devised by Jeremy Bentham where from a central tower any prisoner could potentially be observed without their knowledge. This idea was updated in the 1970s and applied to society in general by philosopher, Michel Foucault. As a metaphor, the panopticon has been applied to surveillance societies, positing the idea that citizens’ behaviours may alter if they believe they may be being watched. Oscar Gandy has labelled this process, “the panoptic sort” whereby subtle manipulation of our behaviour takes place in the knowledge that we may be being observed at all times.

As Nissenbaum has summarised:

*Widespread surveillance and the aggregation and analysis of information enhance the range of influence that powerful actors, such as government agencies, marketers, and potential employees, can have in shaping people's choices and actions.*

Following the Snowden leaks, a number of studies emerged that looked to dissect the force exerted by the perception of surveillance on our online behaviour. Jon Penney of the Oxford Internet Institute undertook a detailed analysis of web traffic to topics on Wikipedia designated by the Department of Homeland Security as related to terrorism. Penney found a 20% drop in traffic following the NSA leaks, with a significant long-term impact that emerged even as press coverage of the leak dissipated. A similar study carried out by Alex Marthews and Catherine E. Tucker into the impact of the Snowden revelations on Google search behaviour for users based in the US and 40 of their trading partners identified a similar chilling effect that was not limited to searches related to national security alone, with a reduction of searches related to issues including health.

Article 19 of the Universal Declaration of Human Rights outlining the right to free expression states that everyone has the right to “seek, receive and impart information and ideas through any media and regardless of frontiers.” As the seeking and obtaining of information increasingly takes place online, the ‘chill’ outlined in both Penney’s study on Wikipedia and Marthews & Tucker’s on Google illustrates a distinct threat to how we understand and realise our right as

---


If people are chilled from informing themselves about breaking news stories and other important news events, or from researching matters of law, security, and public policy related to “terrorism” online, then surveillance-related chilling effects will have serious implications for public deliberation about important topics. With people potentially chilled or deterred from such basic acts of information gathering, people will be less informed and our broader processes of democratic deliberation will be weakened.

Beyond searching and obtaining information, the impact of surveillance continues to shape how we engage with digital spaces. Elizabeth Stoycheff investigated the impact of surveillance on the spiral of silence model, which speaks to the tendency of those who hold minority viewpoints to stay silent when confronted with majority opinions. When exploring Facebook, this phenomenon was enhanced when there was an increased perception of surveillance with individuals refusing to speak up and contribute to the discussions taking place online.

The significance of the different forms of chilling highlighted in these studies speaks to the importance of the Internet in providing free and accessible tools for us to realise our fundamental freedoms including the rights to free expression and free association and conversely the unique threats that are associated with this technology. It is from this basis that this report seeks to further explore the impact of surveillance on the free expression of writers based in Scotland.

---

Piecing together the toolbox

Given the growing research into the impact of surveillance on how we use the Internet for a range of behaviours and activities, it is vital, tools, options or alternatives are available for users to take steps to protect their online security and privacy if they so choose, enabling them to continue to use digital services with key threats mitigated or addressed fully. In this study we phrase this part as that of ‘individual agency’, or whether those surveyed feel they do or do not possess the skills, knowledge or ability to protect themselves against surveillance and conduct their work securely. This issue is deeply connected to technologies known as Privacy-Enhancing Technologies (PET), which are tools that seek to protect online privacy and security both within the tool itself and as part of the device as a whole. This is a complex issue that evolves as technologies do but raises distinct issues as to how individuals contextualise their digital rights and how they develop an awareness as to the tools available to protect themselves.

The move towards identifying and utilising PET makes the complex interplay of our rights and digital service provision tangible; it offers concrete steps that can address a complex and largely unseen issue. There are many challenges relating to PET that can limit the uptake of such technologies, including:

• The perception that these technologies require a high level of technical literacy to use effectively. For example, PGP encryption for email communication requires specific and highly customisable tools to be utilised by both sender and recipient to ensure the tool is effectively deployed;
• The ever-changing nature of these technologies, which means that nothing can guarantee total security or privacy in the future - as technologies evolve the chance that a vulnerability is discovered increases;
• The perception that they are only of use by those with something to hide.

This latter point is an expansion of the ‘nothing to hide, nothing to fear’ mind set that has framed much of the discussion around surveillance, and can be seen in the widely-held public perception of tools such as encryption or Tor (a system that allows anonymous web browsing) as tools solely for criminals. While such usage is clearly a legitimate concern for governments and law enforcement agencies in that these tools can be used to further criminal means including drug and weapon sales, as well as the illicit trade in images depicting child abuse, uses of the same technology support crucial rights and values such as freedom of expression across the globe. For instance, PETs are regularly used by activists, journalists and academics around the world, including in authoritarian regimes, to bypass censorship and overcome information vacuums. The value-neutral nature of these tools has ensured that governance and policy-making around these issues is fraught with challenges. Following a number of terrorist attacks in Manchester and London in 2017, the UK Government has exerted pressure on technology companies to restrict the use of end-to-end encryption for communications apps to give the security services access to content data shared by users across the UK. This position has gained support from other G20 nations as part of their anti-terror strategies, which has arguably reinforced the negative perception of PET, even while these tools are becoming far more widely used – WhatsApp, which is end-to-end encrypted so that only the intended recipient can view the content, is used by...
over a billion people around the world every day\textsuperscript{20}.

The perception of technical complexity is being challenged as PET become more user friendly, deploying a ‘privacy by design’ approach that ensures privacy concerns are addressed as software and hardware is developed, requiring very little modification necessary on behalf of the users. Beyond the tools used by users around the world, there is a requirement that technical literacy is addressed and improved on the user side of this debate. As a great deal of digital development programmes are targeted at basic ICT literacy, such as sending emails and creating a variety of different files or protecting companies against cyber attacks, alongside state-supported infrastructure projects such as Digital Scotland’s work to roll out high speed Internet access across Scotland, with a goal to extend “high speed fibre broadband to around 95% of Scotland by the end of March 2018”\textsuperscript{21} there remains a question as to the services out there to support the awareness and adoption of PETs for interested users across the country that do not come from a technical background. Without this, advocacy for and utilisation of PET is too dependent on civil society organisations with limited resources and geographic coverage and so will be deployed imperfectly, allowing inequalities to frame how people identify and attempt to address their digital threats.

> For instance, PETs are regularly used by activists, journalists and academics around the world, including in authoritarian regimes, to bypass censorship and overcome information vacuums.

In their report, Privacy, Security, and Digital Inequality, the Data & Society Research Institute identified “how technology experiences and resources vary by socioeconomic status, race, and ethnicity” in the US. This study of the privacy and security experiences of low-socioeconomic status populations outlines a significant criticism of the idea that there is one cover-all approach to digital insecurity and privacy threats. In the summary, the findings are outlined as follows:

\textbf{Americans with lower levels of income and education are acutely aware of a range of digital privacy-related harms that could upend their financial, professional, or social wellbeing... there are significant racial disparities when looking at privacy-related concerns; in particular, foreign-born Hispanic adults stand out for both their privacy sensitivities and their desire to learn more about safeguarding their personal information. Yet, many of those who feel most vulnerable to data-related harms also feel as though it would be difficult for them to find the tools and strategies needed to better protect their personal information online.}\textsuperscript{22}

Where individuals source the information and practical tools needed to address their concerns related to the utilisation of digital services in light of enhanced surveillance programmes may colour how the awareness of surveillance (both corporate and state) modifies their behaviour. For example, are you more likely to change your behaviour if, after being made aware of the threats to your online privacy, you know what steps to take to address this concern and where to go to find this information? This continuum from awareness, potential behaviour change and individual agency forms the backbone of the study and establishes a framework within which we can explore the complex interplay of rights, expression, data and the perception

\textsuperscript{21} Digital Scotland. 2017. \url{https://www.scotlandsuperfast.com/}
of surveillance.

About this study

Building on the work undertaken by PEN America, we have deployed a similar methodological approach utilising an anonymous online survey and follow-up interviews with Scottish PEN members and other writers based in Scotland. While many of the same questions remain, leaving open the possibility for a comparative study in other countries in the future, we adapted some questions to ensure the study is relevant to writers based in Scotland, including the addition of questions focused on the Investigatory Powers Act.

Following preliminary analysis of the questionnaire results, we identified several key areas for follow-up questions in interviews that were carried out to add depth and detail to the survey data. We asked participants whether they had been avoiding researching or writing about certain content, and whether they had changed their behaviour as a result of their views and awareness of surveillance. We also asked them about their perceptions of the societal impact of digital surveillance and the potential impact on culture and society of writers’ self-censorship, as well as asking whether participants have or may want to increase their personal privacy and security online.

Several important themes emerged from the interviews that illustrated shared concerns regarding surveillance. These themes related to:

- Freedom of expression and inquiry
- Individual agency
- Individual behaviours
- Perceptions of surveillance

2. METHODOLOGY

The findings in this report are from 118 online survey responses and eight follow up interviews that took place between October 2016 and May 2017. The survey questions are based on those developed by PEN American for their Chilling Effects report in 2013, amended by Scottish PEN and University of Strathclyde researchers to fit the UK context. The final questionnaire contained 21 questions and is provided below (Appendix I).

The survey was publicised through the Scottish PEN mailing list and with key partners. It was available for respondents to complete between October 2016 and January 2017, with regular reminders sent through email and social media promotion. The email provided information about the nature of the questionnaire, a description of its purpose and a link to the Qualtrics questionnaire.

Of the 118 respondents who completed the questionnaire, 62% (n=67) said they were Scottish PEN members, with 65 saying they were writer members and 2 identifying as reader members. 39% (n=42) reported they were not PEN members (total 109 responses out of 118). In terms of roles, 1% (n=1) identified themselves as an agent, 12% (n=19) as an editor, 12% (20) as an educator/academic, 7% (n=11) as a translator, 64% (n=102) as a writer and 4% (=7) as something else (162 total responses, as multiple selections were allowed). Different writing roles included musician/lyricist, poet, essayist, author, copywriter and blogger. Throughout this report we refer to these individuals as ‘respondents’, to acknowledge their different roles and membership statuses.
Within the questionnaire, respondents were asked if they would be willing to take part in follow-up interviews. Of the 36 who indicated that they would be willing to do so, 10 replied to invitations to be interviewed and eight interviews were successfully scheduled and conducted. Interview questions were based on a framework devised by Scottish PEN and researchers at the University of Strathclyde covering key themes emerging from the PEN American Chilling Effects study and the literature around self-censorship. Questions were devised as starters for discussion and unscheduled follow-up questions were asked where appropriate for more information and perspective from respondents. Where the respondents were unable to travel to the University of Strathclyde, interviews were held over Wire, an end-to-end encrypted video chat service.

It is important to acknowledge some limitations of the study. The sample size is relatively small, with the survey response rate representing a small percentage of the overall Scottish PEN membership and the broader writing community in Scotland, alongside a small number of interviews. As a result, it was not possible to identify statistical significance within the data analysis. This is also necessarily a survey of writers who are members of Scottish PEN or involved with a number of partner organisations and therefore not necessarily a reflection of all writers in Scotland. Additionally, the questionnaire was available online only and distributed via a mailing list and social media, as well as being shared to partners, thereby limiting responses to Scottish PEN members and the organisation’s broader network with active email addresses or a social media presence. The responses may be influenced by a responder bias from individuals with an existing interest or concern around issues of surveillance, or those who feel comfortable completing an online survey about online surveillance. Nevertheless, the responses from the questionnaire and data from the interviews provide valuable insight into some of the key concerns of writers and the potential impact of state and corporate surveillance.

3. FINDINGS

Below we present the combined findings from our survey and interviews. Together they paint a picture of the impact of surveillance on writers’ attitudes and behaviours. It is broken down into four sections:

- Writers’ perceptions of freedom of expression and inquiry and the impact surveillance has on these, which provides insight into writers’ views about the value of freedom of expression and the ways in which surveillance may pose a threat to it;
- Writers’ perceptions of surveillance, which describes respondents’ views on government and corporate surveillance;
- The impact of surveillance on writers’ behaviour, which details the ways in which writers feel their behaviours will change, or have already changed;
- Individual agency, in which we discuss the ways in which writers feel they do or do not possess the skills and abilities to protect themselves against surveillance and conduct their work safely and securely.

Writers’ perceptions of freedom of expression and inquiry, and the impact of surveillance

Perhaps unsurprisingly, given the interview subjects were all writers, freedom of expression was an important consideration. Further to this, there was an acknowledgement expressed that the intersection between one person’s freedom to express themselves can often impinge on the rights of others:

I mean something we haven’t talked about at all are boundaries between free expression and pornography, for example, or free expression and
then encouraging behaviour that impinges on other people’s freedoms. And I think that’s where it gets really quite problematic (Respondent One).

Respondent Eight acknowledged that the right to privacy, which supports freedom of expression and inquiry, also poses a challenge: “privacy...in the sense of the citizen, is the ability to get on and say pretty much whatever you want, except if it has ramifications which can physically harm the rest of society, I suppose.”

Going further Respondent One suggested:

*We claim in PEN to be an ethical body, you know, and have an ethical view of how people should treat each other. I don’t think we would – I would hope PEN wouldn’t support the rights of people to assert that other people should be locked up for expressing their opinions, and yet the opinion that someone should be locked up for expressing their opinion is itself an opinion. So how do you balance this?*

With regards to how surveillance might impact on the right to free expression, Respondent One argued:

*What are they expressing? That has to be the question. What do they want to express that they might change because of the surveillance? What could they express before that was acceptable that they can’t express now because of the surveillance? Is that not the question? It’s not the surveillance that’s significant, it’s what people want to say.*

The significance of the content expressed appears to play a distinct role in understanding the potential impact of surveillance. Jon Penney’s study on Wikipedia usage and Alex Marthews and Catherine E. Tucker’s on Google search behaviour both used terms identified by the Department of Homeland Security as part of their social media-monitoring programme, which included terms such as “suicide attack”, “nuclear enrichment” and “eco-terrorism”23. So while these studies only explored self-censorship in relation to terms that carried a great deal of significance in terms of divisive and complex issues such as terrorism, they highlight a complex interplay between specific topics and self-censorship. The Marthews and Tucker study also found that Google users were deterred from searching for topics related to their health, demonstrating a distinct threat for people seeking out advice online.

---

Respondent Three also offered that:

I think I would avoid direct research on issues to do with Islamic fundamentalism. I might work on aspects of the theory, but not on interviewing people and that, whereas in the past, I have interviewed people who would be called, in inverted commas, “subversives”.

Respondent Two also suggested some areas they felt were potentially controversial and likely to attract attention:

I was writing something about rape, rape featured in it, it was the crime at the centre of what was then a crime novel. That’s changed, the plan for that book has changed, and not as a result of this. But I was looking at statistical analysis, I was looking at reports of rape in prison, I was looking at this, I was looking at that, and I’ve just stopped doing that, because I think as a theme, it’s far too edgy, it’s far too out there, and I don’t want people tracking me and what I do in this sense, or any other sense, really.

Respondent Six intimated similar concerns:

Yeah…obviously anything to do with children I’d be, certainly take a long think about it before just jumping in and researching anything to do with that. I haven’t really written about children yet, so it’s one that’s always on my agenda. So certainly, anything to do with children, I’d be very, very wary of researching that online. I seem to recall there was an incident, ooh, quite a few years ago with Pete Townshend of a similar thing, he had some dubious material on his computer and it was research for a book, apparently. Yeah, I’d definitely be a bit dodgy, I think researching anything to do with child abuse, you’d be very wary – I don’t think I’d be happy to do that online.

The respondents intimated potentially controversial areas that were of both political and societal concern that they perceived as likely to draw attention to their activities. If the choices outlined by the respondents here are indicative of a broader topic selection process undertaken by many writers, we could have a number of important topics largely ignored by writers to ensure they are not increasing the possibility of surveillance. When key issues are ignored, we may be left with a homogenised literary or journalistic landscape, with silence on a number of vital issues.

When key issues are ignored, we may be left with a homogenised literary or journalistic landscape, with silence on a number of vital issues.

Respondent Seven highlighted that they have found value in writing about contemporary topics but placing them in an historical setting:

I mean, recently I’ve written a piece that I would have felt uncomfortable writing as a contemporary piece in…this geographic location, but writing it as a historical piece in a different real-world location, if you will, has made it an easier piece to write. So I’m still writing about the same stuff…but, you know…taking the incredible step of, as a fiction writer, writing it as a fiction, you know?

“Acceptability” or the idea that certain topics could affect the likelihood of increased data collection appeared to bring to light a complex relationship between the writer and the political and cultural environment within which they expressed themselves. As highlighted by Respondent Four, the basis of this relationship was far from clearly established or fixed, with what is and is not acceptable to express in terms of how government ideologies are liable to change over time:
I think one thing that people don’t ever seem to give any consideration to — governments certainly don’t, they always say, “Oh, well, if you’ve done nothing wrong, you’ve got nothing to fear, blah-blah-blah”: they don’t consider that the ideologies of governments can change, and what might be perfectly acceptable in one era, or even a decade or so ago, might become unacceptable in a future era or future ten years, even, and people might be... for want of a better word, spied on, for views that were perfectly OK before and are no longer OK.

Elaborating further, Respondent Four highlighted how in times of war or conflict, acceptable behaviour can change very quickly into something deemed inappropriate or even dangerous:

But it’s very easy, once people are jittery — and that’s why I said also that war is a time when that particularly happens — that the most innocent behaviour can look, you know, suspicious.

With the distinction between war time and peace time becoming harder to define as military engagement has continued, following World War II and the 9/11 terror attacks, in a number of smaller and less well-defined theatres around the world, as well as the increase of non-nation state terror attacks and remote warfare, how our perception of what tools should be available to the state, in what contexts, and how this access affects our fundamental freedoms remains a complex issue that falls outside the scope of this study, but remains a key topic of further exploration.

Writers’ perceptions of surveillance

The following section details respondents’ views about government and corporate surveillance, from both the questionnaire and interview data.

There is widespread concern among writers about government surveillance. The majority of writers surveyed reported that they are following news stories about government surveillance efforts within the UK very closely (17%) or somewhat closely (59%). The majority said they are worried about current levels of government surveillance of Britons, with 32% saying they are very worried and 56% said they are somewhat worried (88% total). No respondents reported that they were not worried at all about government surveillance.

There is concern about corporate and state surveillance in various forms:

• 74% say they are very concerned and 20% say they are somewhat concerned about the UK government’s new law (the Investigatory Powers Act) to collect and analyse data and metadata (e.g. time and location) on e-mails, browsing and other online activity of Britons (94% total);

How concerned are you by the UK government’s new law (the Investigatory Powers Act) to collect and analyse data and metadata on e-mails, browsing and other online activity of Britons?

Very concerned (74.36%)
Somewhat concerned (19.66%)
Not too concerned (0.85%)
Not concerned at all (0.85%)
Not sure / not applicable (4.27%)
• 82% say they are very concerned and 15% say they are somewhat concerned about technology companies being compelled to work with the government to provide vast amounts of personal information on Britons (97% total);

• 79% say they are very concerned and 18% say they are somewhat concerned about the UK government secretly accessing journalists’ call records (97% total);

How concerned are you by technology companies being compelled to work with the government to provide personal information on Britons?

- Very concerned (82.1%)
- Somewhat concerned (14.5%)
- Not too concerned (0.9%)
- Not concerned at all (0.9%)
- Not sure / not applicable (1.7%)

• 52% say they are very concerned and 36% say they are somewhat concerned about corporations gathering data to track and analyse consumer behaviour and preferences (88% total);

• 87% say they are very concerned and 9% say they are somewhat concerned about suppression of free speech and press freedom in countries other than the UK (96% total).

How concerned are you by corporations gathering data to track and analyse consumer behaviour and preferences?

- Very concerned (52.14%)
- Somewhat concerned (35.90%)
- Not too concerned (8.55%)
- Not concerned at all (2.56%)
- Not sure / not applicable (0.85%)

Overall, there is concern around the governments’ priorities around surveillance. The majority of respondents (56%) reject the view that the government’s primary concern is monitoring communication with foreigners and that it is not really interested in domestic surveillance. A third (33%) of respondents reported that the statement “I have never been as worried about privacy rights and freedom of expression as I am today” reflected their concerns very or somewhat closely.

Overall, there is disapproval with regard to the government’s approach to the collection of Internet data for anti-terrorism efforts. 55% said they disapprove of the government’s collection of Internet data, with 27% reporting they did not know whether they approved or disapproved. Only 19% approved of the government’s collection of Internet data as part of anti-terrorism efforts.
Respondents questioned whether widespread data surveillance is essential for states. Over half (52%) of survey respondents rejected the view that “surveillance is something all governments do – there’s really nothing new or worrisome about what’s happening now”. Additionally, only 11% of survey respondents very or somewhat closely agreed with the statement that “widespread data surveillance is an absolutely essential tool for the government in the fight against terrorism” – over half (52%) disagreed with this statement.

These mixed perceptions were reflected in the responses to the interviews. There was acknowledgement from some respondents that some surveillance was inevitable and perhaps necessary. Respondent Three offered that:

*I accept that there is a trade-off between high levels of personal privacy stroke security and the security of the community... It’s accepting that it’s going to be collected, I think. I think the fundamentalists who say it shouldn’t be collected are foolish. It’s the old classic, I mean, it’s the extreme civil rights argument or civic rights argument, and I think that doesn’t work. I think it’s very difficult in modern complex societies. So I think that’s the first thing, that we have to accept that this is going on.*

Respondent Four offered a similar sentiment that surveillance in itself may be a necessary activity, but suggested it is what is done with the data that is the true danger:

*Because clearly, if you think of things like, ordinary things like surveillance cameras, things like that, their primary purpose, undoubtedly, is to try and reassure people, to keep people safe, to record behaviour that’s criminal, and you can’t – even though one might feel uncomfortable about that – say that in itself is necessarily worrying. It’s not the taking of information, perhaps, so much as what’s done with the information that’s taken.*

Echoing this sentiment, survey respondents expressed concern that what is done with the data may not be secure or safe: Over a third (35%) of respondents expressed concern that “personal data collected by
the government will be vulnerable to abuse for many years because it may never be completely erased or safeguarded”. A third (33%) of respondents very or somewhat closely related to the statement “I am worried that a vast amount of data will be in the government hands and vulnerable to bureaucratic bungling, misuse, and partisan abuse”.

In the UK, these concerns are significant following the passing of the Investigatory Powers Act, which will require both state agencies and private companies to hold a great deal of personally identifiable data to supplement and support the state’s security processes. Following the TalkTalk hack in 2015 where data of over four million customers\textsuperscript{24} were accessed by unknown third parties alongside the increase in known cyber attacks in both the private and public sector, the ability of organisations to hold data securely will directly impact public trust and thusly their support of the surveillance powers outlined above.

Beyond the trust derived from agencies holding data securely, how data is used similarly contributes to public support for known surveillance programmes. In a legal challenge against the UK government, documents released by Privacy International revealed the trivial uses of data held by the intelligence agencies. In a memo released during the hearing, the Secret Intelligence Agency (SIS) stated that intelligence analysts utilised databases for the goal of “looking up addresses in order to send birthday cards, checking passport details to organize personal travel, checking details of family members for personal convenience.”\textsuperscript{25}

A common observation offered from several respondents was that responsible surveillance was a “balancing act” between preserving rights and impacting on them. This fed into several observations around what the justification for surveillance was. Respondent Three offered that: “In terms of government, my argument would be that governments need to take much more seriously the concerns that individuals and groups have about the potential of intruding.”

In a similar vein, Respondent One offered that, “I don’t really have a problem with the Special Branch finding people who are planning terrorist attacks. I think, you know, you find very few people have a problem with that, OK?” Nevertheless, Respondent One clearly argued that the concept of harm to society had to be clearly stipulated to justify surveillance on individuals:

\textit{It should be just as worrying, I think, really, if you end up on a blacklist because you hold views that are not very savoury – unless they are actually inciting to violence and hatred, then of course, obviously, you’re breaking the law – but simply to oppose something without breaking the law shouldn’t make you a target for surveillance, I think.}

This issue regarding the threshold of surveillance powers being tied to illegality speaks to the core of the Snowden revelations that revealed the bulk powers at the heart of the surveillance powers of the 5-eyes countries, which sought data on the many to find the few. Theresa May (both as Home Secretary and Prime Minister) expanded on this concept stating “if you are searching for the needle in the haystack, you have to have a haystack in the first place”.\textsuperscript{26} What has been ignored from this position is that the make up of the ‘haystack’ is not unlawful content but the data generated by the population at large. As data generation at scale is

\begin{itemize}
\end{itemize}
the foundation of the digital economy, how the data that is created from our daily interactions online is used, beyond our consent or knowledge, as part of state mechanisms including anti-terrorism and crime prevention strategies raises concerns related to the proportionality of these powers and how they may affect broader online engagement.

In terms of the impact of surveillance on writers, over three quarters (79%) of respondents believe that the statement “Increased government surveillance is especially harmful to writers because it impinges upon the privacy they need to create freely” reflected their views very (46%) or somewhat closely (33%).

How closely does this statement reflect your opinion: Increased government surveillance is especially harmful to writers because it impinges upon the privacy they need to create freely

- Very close (45.7%)
- Somewhat close (32.8%)
- Not too close (12.9%)
- Not close at all (5.2%)
- Not sure / not applicable (3.4%)

In the interviews, Respondent Eight expressed fear around the powers of the Investigatory Powers Act and its impact on the writing profession:

So, for me, the power of the state, what the bill does in giving the power of the state the ability to have limitless prosecution of writers is incredibly scary and actually very close to what’s happening in Egypt or what has happened in Egypt, actually. It seems hyperbolic to say that, but it is very close to that, because you have this near-total power for state institutions to impress their will upon individual writers.

They continued that:

Now, that’s...that feels like a violation of my purpose. You can’t exist as a writer if you’re self-censoring, if you’re thinking about a law that’s come into effect which forces you to self-censor because you don’t want to go to jail because you know that actually there isn’t the public support; not only there isn’t the legal support for you to operate, there isn’t actually the popular and cultural support for you to operate as a writer. Because, again, I can’t emphasise this enough, that this bill is the legal embodiment of a cultural tendency that’s happened over the last, say, 20 years.
The increasing impact of state surveillance on the ability of a writer to do their job was clearly a worry expressed in the findings from the interviews. The broader societal impact of surveillance from pervasive surveillance was also argued to be of concern. Respondent Three suggested that: “I think at the wider level, I have much graver concerns there. I think a lot of the societal impact or cultural impact is indirect.” Respondent Two in a similar vein suggested that it had “huge implications for us, and in all sorts of walks of life.”

Respondent Three recalled actually destroying a book on seeing someone who possessed it being prosecuted: “I realised about a year ago that somebody was actually arrested and charged with possession of The Anarchists’ Cookbook. And I destroyed it: I just put it through the shredder.”

Perhaps tellingly, Respondent Two offered that: “I suppose it’s pointing towards self-censorship being the norm, and I expect that’s already happening.”

The impact of surveillance on writers’ behaviour

Writers reported that increased government surveillance activity would make them use the Internet differently to communicate, research and work.

- The majority of respondents said that the collection of metadata (39%), collection of content data (62%), hacking platforms, networks or devices (60%), and installing backdoors into encrypted platforms (59%) would make them use the Internet differently. 45% reported that undermining end-to-end encryption would make them use the Internet differently.
- Only 6% reported that none of the above would make them use the Internet differently.

What government activity might make you use the Internet differently to communicate, research or work?

- Collection of metadata (13.6%)
- Collection of content data (21.7%)
- Hacking platforms, networks or devices (20.8%)
- Installing backdoors into encrypted platforms (20.5%)
- Undermining end-to-end encryption (15.7%)
- None of the above (5.6%)
- Other (please specify) (2.1%)
Writers reported that their behaviour around communicating, researching and working would change in significant ways if the government collected metadata or content data, hacked platforms, networks or devices, installed encryption backdoors or undermined end-to-end encryption (quotes are taken from survey responses):

- 20% said they would consider using the Internet and other online tools less frequently and stop using them altogether, saying “I’d be more concerned about doing certain things online” and “I would stop using the Internet for anything more than routine exchange and business”;
- 12% said they would engage in self-censorship, becoming less open and truthful and more guarded in what they communicated in their work and what they shared publicly, saying “I might be more cautious in sending or writing material which could be misconstrued in an atmosphere of paranoia”, “no political thinking on social media, perhaps” and “thought and expression would be heavily edited and less me”;
- 9% said they would do less searching or avoid researching or searching for information about particular topics, saying: “I would think twice about certain aspects of research”.
- 9% said they would take steps to increase their online privacy and security, for example by using a VPN, proxies and encryption;
- 3% said they would take steps to hide or obscure their identity online;
- One respondent said they may stop communicating with people in order to protect them: “I might be cautious about who I was seen to be communicating with in case it caused problems for them.”
- One respondent said they would increase their Internet use in order to add to the data burden.

In many cases writers are already engaging in self-protective behaviour that is limiting their freedom to research and write freely, both publicly and privately, with respondents reporting:

- “I avoid searching for and reading about certain topics”
- “I am extremely careful now about what I Google for research”
- “I generally feel I am developing an unwelcome ‘inner censor’ on what I write and what I research”
- “I am much more circumspect about what I put into emails”
- “I now cover the video camera on my computer, for example”

Writers reported self-censoring and actively changing or considering changing their behaviour because they think the government may be monitoring their communications. Respondents reported that they had considered doing or already had done the following:

- Curtailed or avoided activities on social media- 28% have done this and 13% have seriously considered it (41% total)
- Avoided writing or speaking on a particular topic – 22% have done this and 17% have seriously considered it (39% total)
- Deliberately steered clear of certain topics in personal phone conversations or e-mail messages – 20% have done this and 17% have seriously considered it (37% total)
- Refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious – 16% have done this and
20% have seriously considered it (36% total)

• Taken extra steps to cover or disguise digital footprints – 13% have done this and 16% have seriously considered it (29% total)

• Taken extra precautions to protect the anonymity of sources – 18% have done this and 10% have seriously considered it (29% total)

Avoided writing or speaking on a particular topic – 22% have done this and 17% have seriously considered it

Changes in behaviour identified by writers as a result of concerns around surveillance include self-censorship of research, writing and speaking:

The decision to change online behaviour, or avoid online tools altogether, intersects with what topics writers decide to cover in their work as outlined in the previous chapter. In 2014, the Pew Research Center outlined that 86% of Americans were willing to have an in-person conversation about the NSA Snowden revelations, but just 42% of Facebook and Twitter users were willing to post about it on those platforms.27

Survey respondents also reported avoiding writing or speaking about particular subjects that they thought could make them a target of surveillance. Writers reported changing what they say and how they say it in various ways, including: abandoning research on unwritten stories; finding alternative language to discuss topics and avoid attention; toning down their writing and communication; becoming wary of how humour may be conveyed and avoiding flippancy; and considering more carefully what to post online. This finding is inline with PEN America’s study in 2013 which outlined that 1 in 6 writers avoided ‘writing or speaking on a topic they thought would subject them to surveillance’.

Over the past year or two, have you personally done or seriously considered doing any of the following because you thought your communications might be monitored in some way by the government?

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>No, I have not (%)</th>
<th>Have seriously considered (%)</th>
<th>Yes, I have (%)</th>
<th>Not sure / Not applicable (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avoided writing or speaking on a particular topic</td>
<td>57.8</td>
<td>17.2</td>
<td>21.5</td>
<td>3.4</td>
</tr>
<tr>
<td>2</td>
<td>Curtailed or avoided activities on social media (e.g. Facebook, Twitter)</td>
<td>48.3</td>
<td>12.9</td>
<td>27.6</td>
<td>11.2</td>
</tr>
<tr>
<td>3</td>
<td>Declined opportunities to meet – physically or electronically – people who might be deemed security threats by the UK government</td>
<td>71.6</td>
<td>5.2</td>
<td>-</td>
<td>23.3</td>
</tr>
<tr>
<td>4</td>
<td>Deliberately steered clear of certain topics in personal phone conversations or e-mail messages</td>
<td>60.0</td>
<td>16.5</td>
<td>20.0</td>
<td>3.5</td>
</tr>
<tr>
<td>5</td>
<td>Refrained from conducting internet searches or visiting websites on topics that may be considered controversial or suspicious</td>
<td>54.3</td>
<td>19.8</td>
<td>16.4</td>
<td>9.5</td>
</tr>
<tr>
<td>6</td>
<td>Changed or stopped work on specific projects due to increased perception of surveillance</td>
<td>78.3</td>
<td>8.7</td>
<td>4.3</td>
<td>8.7</td>
</tr>
<tr>
<td>7</td>
<td>Taken extra precautions to protect the anonymity of sources or others you may have communicated with</td>
<td>56.0</td>
<td>10.3</td>
<td>18.1</td>
<td>15.5</td>
</tr>
<tr>
<td>8</td>
<td>Taken extra steps to cover or disguise digital footprints (e.g. used stronger encryption software, changed to more secure digital service provider)</td>
<td>62.1</td>
<td>15.5</td>
<td>12.9</td>
<td>9.5</td>
</tr>
</tbody>
</table>
Interviews yielded more depth around the impact of surveillance on writers’ behaviour. In terms of how surveillance has or has not changed the behaviour of writers, there were mixed observations from the respondents. Respondent One suggested that, “I don’t think we’re censoring ourselves because of surveillance.” Respondent Seven took a similar stance, offering that they had, “made a wilful decision to continue to write in a way that almost pretends that that doesn’t happen.” However, they did acknowledge what they perceived as a changed culture, but felt that adhering to an ethical stance to their profession was vital:

“I think post-Snowden and...particularly in the advent of the Trump presidency and the reports that they will be looking to take up password information, social media information and email information to get into the country, did give me pause, but again, I’ve decided it’s more important to follow the dictates of my art than it is to let, so self-censor, essentially.

This is an important recurring theme that raises concerns when we explore what forces encourage or dissuade expression. While many individual writers are able to resist the urge to self-censor themselves, or believe themselves to have the necessary protections to enable them to express themselves, this cannot be assumed to be the case for writers as a whole. Being able to publish free from perceived threats requires the knowledge and existence of a number of factors beyond the writer’s control including legal protections, an established pluralist media and cultural landscape and other support mechanisms. This may not be the case for writers who come from or represent vulnerable or marginalised groups including asylum seekers and refugees, members of the LGBTQ community, women, ethnic minorities and opposition writers. To this end, the choice to self-censor, while being a choice each writer has to make, is not an equal choice available to all and remains a distinct threat to the writing community both in Scotland and beyond.

The choice to self-censor, while being a choice each writer has to make, is not an equal choice available to all and remains a distinct threat to the writing community both in Scotland and beyond.

The choice to self-censor yourself is not a uniform reaction. It is coloured by levels of confidence in what you have to say, existing or potential vulnerabilities that may be exacerbated by expressing yourself, as well as the perceived efficacy of available protections and methods of recourse. In a follow up to his 2016 study, Jon Penney surveyed over 1,200 US-based adult Internet users to “explore multiple dimensions of chilling effects online”28, which included state and corporate surveillance, the receipt of legal notices as part of online regulatory systems (such as the Digital Millennium Copyright Act (DMCA)), cyber bullying and trolling. The significance of this study was the ability to identify demographic differences in terms of the willingness to self-censor activity online.

Penney found that young people—“the younger the participant, the greater the chilling effect”29— and women are more likely to self-censor themselves when confronted with surveillance, legal notices or episodes of cyber bullying. While this study was not focused on surveillance alone – “gender had no effect in the second (government surveillance) scenario”30, although

29 Ibid.
corporate surveillance had a greater impact on women – how self-censorship manifests online will frame how we utilise online tools for a range of behaviours and to what extent we are willing to change our behaviour or seek out tools or practices to address a range of different threats.

Respondent Three also revealed that their “consciousness of being surveilled is much more heightened” and that this was “based on the wider issues of realising that governments and various agencies have the ability to eavesdrop on you in what you’re doing; I mean, also, there are so many intrusive activities available.”

As outlined in a previous chapter, the choice to avoid certain topics to research or write about, alongside how willing people are to express themselves at all, there is also an impact on how people participate in broader discussions, both online and off. Respondent Three suggested that it did not necessarily influence what they wrote about, but did so when it came to potential interventions in debates:

> It doesn’t make me cautious about what I write, but it does make me more cautious about where I’d intervene. So, you know, I’d think very carefully about how I would write an article for a newspaper if I was invited to do so.

Free expression extends beyond what is written in novels, academic publications or journalistic output. So investigation into the impact of surveillance on expression should reach beyond the creative output, exploring how self-censorship impacts every facet of expression including media output, social media usage and other forms of expression. The Spiral of Silence model as outlined by Elizabeth Stoycheff in her piece on online involvement highlights how the perception of surveillance can further dissuade expression from those who hold minority opinions. As minority opinion holders already struggle to get their voices heard on the increasingly polarised and homogenised ‘spheres’ of communication found online, how surveillance affects this form of expression, beyond formalised publications, speaks to the broader impact on expression that could be overlooked through a formalised publication-based approach.

Within the publishing industry this form of ‘informal’ online expression that includes but is not limited to op-ed writing, social media, blogging and podcasts is growing in significance due to new models of promotion and marketing that is identified as ‘digital-first’. With this new responsibility for writers, editors and publishers to participate in online marketing efforts, we need to understand how external forces such as the perception of surveillance can shape this form of associated expression as they may be underpinned by similar concerns as formally published work, including the need to research and communicate online.

Awareness of surveillance had led to some new behaviours among some interview respondents. The use of “traditional” sources of information seemed to be of re-discovered importance for some: “I’m maybe changing the paths to the research. So I’ll maybe go look things up in a book, maybe in the library, for example, rather than just a quick five minutes online to have a look” (Respondent Six). Similarly, Respondent Two stated that, “I think I’ll have to go libraries now”.

Respondent Eight highlighted the importance they felt in keeping work being undertaken separate from any technologies that may store personal or private information:

> So these are all the kind of things, especially when it comes to languages, but also investing in new technology and sort of separate devices, as well, and just making sure there’s a clear barrier between your personal life and your private life as well.
In the context of surveillance outside of the UK itself, Respondent Seven offered that:

*I will be travelling to the United States later this year, and I am trying to figure out what protections I want to take with respect to my phone and any other electronics I take with me on that trip. I suspect...I’ll end up taking a temporary and/or spare phone with different numbers, different apps on it and all that sort of stuff.*

Respondent Two highlighted an example of self-censorship after the fact while using social media:

*Yesterday on Facebook I posted something that was less than praising or praiseworthy of Theresa May, and I went home, and I thought about it, and I took it down, because I thought, “Really, I just don’t” – you know, it may seem daft, but I’m much more alert to that kind of digital trail now, and how it may be interpreted by whoever in the light of, you know, reactions to the London attacks yesterday, for example.*

Protections exist within UK legislation to protect people who express themselves in a robust or ‘daft’ manner, short of a range of established laws including those protecting against hate speech and malicious communication. If the perception of surveillance establishes a lower threshold than existing laws that encourages people to silence themselves, civil discourse may be significantly weakened as a result.

*If the perception of surveillance establishes a lower threshold than existing laws that encourages people to silence themselves, civil discourse may be significantly weakened as a result.*

Summarising their use of the Internet more broadly, Respondent Two offered: “So maybe I look less, simply, and just use the Internet less.”

**Individual agency**

Agency refers to the capacity of individuals to make decisions about their behaviour and act on situations. This was an area of consideration in the interview because questionnaire responses indicated that respondents were not always confident they had the skills and abilities to protect their privacy and security if they wanted to. Themes around individual agency related to how writers may need to be informed about how surveillance is undertaken and what skills and knowledge they may need to undertake their work in that kind of environment.

**Survey data indicated some concern about public awareness and concern around surveillance.**

Over a third (37%) of survey respondents felt that the statement “most Britons are unconcerned and uninformed about government surveillance” reflected their views very or somewhat closely.

**Survey respondents reported avoiding Internet search tools, email, and online communication tools for fear that their search terms and conversations would be monitored.** Writers reported changing how they use technology, including: using a proxy and VPNs; avoiding work email to communicate with sensitive sources; using more secure and encrypted email providers, search engines, browsers (Tor) and SMS services; using stronger passwords; avoiding insecure websites; disabling cookies; refraining from or reducing use of social media, including Facebook and Twitter; and avoiding the use of electronic communication entirely.

However, there was an acknowledgment from several interview respondents that their awareness of how their use of modern technologies might leave a trail was perhaps lacking.

**Several writers reported that although they have...**
concerns about surveillance, they do not know how they can change their behaviour to increase their privacy and security. For example, one respondent said that they “don’t really understand what most of the above [options] mean”. Another said “I would need to speak to an expert to see how to safeguard my interests”. Others said they “don’t know enough” and “have no idea how to use the Internet ‘differently’”. The significance of these concerns are manifold. As publishing moves more and more towards a digital process from writing, researching, editing and publishing, if writers do not know the tools needed to secure themselves online they may continue to use these tools in an insecure manner or may choose to avoid these tools all together, therefore limiting their chances to interact in a manner that is in keeping with the developments in the field more broadly. In this manner, there are concerns that the establishment of a higher threshold of technical literacy to enable writers to express themselves will alienate many who want to express themselves but are unable to reach that threshold, thereby restricting their ability to take part in the manner they choose.

Respondent One indicated that, “whatever you research, you’re going to leave a trail. So, that I need to learn more about”. In the context of the Investigatory Powers Act, Respondent One also offered that:

I need to learn more about what the implications of the Act are going to be. That’s what none of us know yet, in order to be able to protect myself and in order to be able to do what I want to do digitally.

If writers do not know the tools needed to secure themselves online they may continue to use these tools in an insecure manner or may choose to avoid these tools all together

In terms of how a writer might cover their tracks to be less visible to surveillance techniques, writers expressed a range of views and levels of knowledge. In the interviews, Respondent Three offered that, “I certainly have to think about the technology every time I use it.” Respondent Five suggested:

I think probably what worries me, and probably people my kind of age, would be...does our ignorance of what’s technologically possible and what’s unethically being done, legally or illegally but either of it unethically, make us vulnerable, because we just don’t really understand.

Respondent Five continued that:

A lot of the language of computing, although I’ve been in classes where it’s discussed by experts, just kind of baffles me, to be honest, and...I think probably I need to get educated a wee bit more by someone...because I think we probably are a bit exposed and a wee bit vulnerable, more than we realise. I guess it’s that that’s, I’m obviously not losing sleep over it, but I think I’m a bit more agitated about this.

Where writers might find support for this kind of education was also a key concern. The support of other writers who are knowledgeable seemed to be important:

I have a wider group of people that it’s a closed group that I’m a member of, where people always, if you go on and say, “Look, I’m thinking about this,” there’ll always be somebody who’ll come back and say, “You should look at this program,” or, “I’ll come and have a look at your computer for you,” whatever like that (Respondent Three)

Respondent Eight recognised the knowledge that writers working in areas of the world where surveillance has been a consideration for a longer period of time bring to the profession:
I didn’t actually go to any sort of official sources, whether it was the NUJ or union representation, or even other investigative journalists in Scotland. I actually went to friends that I knew working at BBC Persia, Persian Service, just because a lot of them had experience of graduating as journalists in Iran during the 80s, where things were – you know, they’re still quite bad in terms of freedom of speech there, but things were really, really intense. So I kind of learnt from them.

Respondent Six highlighted that some writers are perhaps not as up-to-date with the issues as they could be:

> I guess it depends how technology-proficient you are. Some people just absorb it, myself, for example, I don’t really worry too much about that in isolation; I just tend to look at the bigger picture, but I do know a few people who are...less literate with IT and for them, it would be a much bigger issue.

When discussing issues around writers’ agency, Respondent Five focused on dissemination of advice to writers by organisations such as PEN as being vital to allow writers to understand the challenges they face in a world with increasing surveillance:

> I think it would be good, I mean, if, for example, the outcome of your study, the Scottish PEN study, was...a leaflet or a booklet or some kind of communication giving advice and tips and suggestions, I would be absolutely delighted, but I don’t know if that’s likely to happen. Or if there was some sort of recommendation, because I think we are...a bit blind.

In this context, agency is deeply connected to digital and technological literacy, which will inform how aware writers are of potential vulnerabilities and potential steps they can take to rectify a problematic or threatening situation. Without this form of literacy, many writers may either avoid certain topics, tools or approaches because they cannot guarantee their security and/or privacy or decide to continue irrespective of known or unknown threats, which can open themselves up to increased data collection or surveillance without their knowledge. While PETs have grown in availability and accessibility (such as end-to-end encrypted chat app, Signal or Tor, the anonymous network) there remains a great deal of work needed to be done to offer these tools to everyday Internet users at the expense of more popular but more insecure tools.

This work represents a key part of the challenge in relation to digital free expression and human rights more broadly, that of breaking down the silos between civil society members, journalists, technologists, policy makers and academics to ensure each discipline can reach audiences and stakeholders beyond their own environment. Enabling those in need, including writers and members of marginalised groups, to positively address their deficiencies in terms of digital literacy requires a multi-stakeholder approach that examines this issue from a range of points of view including technological, legal and academic.

4. CONCLUSION

The impact of surveillance on free expression is a complex issue that only grows in complexity as digital surveillance and data collection continues to grow and define our age. This study is only a snapshot into how surveillance, left unchecked, can undermine the willingness or ability of individuals within civil society in Scotland to give voice to their beliefs and ideas on a range of platforms, both online and off.

While the relationship between surveillance and the full realisation of our fundamental freedoms is ever-
changing, with higher levels of awareness of the capacity of state and corporate surveillance mechanisms, alongside increased academic research on these topics we cannot discount the extent to which surveillance exerts a significant pressure on our fundamental freedoms, whether that relates to how we express ourselves, communicate with others or participate in a myriad of ways online. While it may be hard to draw a direct line between one and the other, we believe the relationship cannot be ignored.

We cannot discount the extent to which surveillance exerts a significant pressure on our fundamental freedoms, whether that relates to how we express ourselves, communicate with others or participate in a myriad of ways online.

This snapshot study highlights a growing concern within writers based in Scotland that surveillance, or the perception of surveillance, is exerting a force on their creative output in a wide variety of ways. The use of the Internet is not limited to the writing and publishing of work alone, establishing itself as an invaluable tool for research, proofing and communicating with a broad range of other stakeholders. To understand this we need to look at the entire process beyond that of publication alone. This complex and deeply subjective creative process offers a number of vulnerable points within which expression, or the potential of future expression, could be discouraged. The chilling of free expression does not manifest solely in the refusal to publish, it can encourage smaller, but no less disruptive, acts of mitigation including avoiding certain sources of information and tools, modifying the tone, setting and language used, as well as limiting participation in all associated work including promotion, communicating with readers and other writers and contributing to civic discourse in a personal context.

Surveillance is, by its very nature, an opaque and secretive tool available to both state and non-state actors. We have no way of knowing to what extent the respondents have experienced actual surveillance but a key point that emerged from this study is that personal experience of surveillance is not required to feel its impact. When we look at the perception of surveillance, as opposed to the experience of actual surveillance, we return to the idea of the Panopticon. It was not being watched that modified behaviour, it was the possibility that the inmates, at any time, could be monitored. Without knowing for sure, the uncertainty was enough to change behaviour even when, without their knowledge, the watchtower was unstaffed. This distinction is of vital importance as we look to explore the impact of surveillance on the realisation of our human rights; by removing the need to prove a direct link to actual surveillance, we can approach this as a largely unexplored part of our modern society that frames our collective experience as opposed to experiences limited to smaller groups. This is not to say that the impact of surveillance is equally felt by every demographic, if state surveillance is a tool used to achieve political goals it will adversely affect members of the community who are, at the time, of interest to the state.

The 2013 PEN America study was a ground-breaking study that attempted to frame the debate and outline key concerns for the written word in the digital age. Self-censorship is a hard behaviour to quantify. Without signalling a choice not to publish, what is unpublished remains hidden from view, with the wider public unable to know what has been censored. Understanding potential drivers to self-censorship can help us identify which situations may make this form of censorship more likely and thus establish protections to ensure people can fully realise their right to free expression. While limited in scale, this study adds to a growing body of research addressing the unseen impact of surveillance on writers beyond that of journalists or political writers alone; it affects writers from a range of backgrounds,
genres, approaches and disciplines in a number of discrete and meaningful ways that warrants further analysis and investigation.

This awareness prompts a need for action. This report highlights a number of meaningful ways we can seek to address the concerns highlighted by the respondents.

Whether this is improving how policy developments are communicated to the public, with robust and inclusive methods by which they can get involved, or through improved programmes for writers and civil society more broadly to understand the privacy impact of big data, as well as steps they can take to protect themselves, we are at a pivotal point in relation to how data generation, collection, ownership and sharing frames our life, both on and offline. With big data increasingly being incorporated within public and private service provision, as well as the emergence of Internet-enabled appliances, the so-called Internet of Things, we need to ensure that all human rights protections remain relevant and robust enough to continue to protect us.

5. PRELIMINARY RECOMMENDATIONS

Recommendations for UK Government

Given the implications of this survey and the passage of the Investigatory Powers Act, Scottish PEN calls on the UK government to take immediate steps to restore public confidence that their privacy is protected both online and off:

1. Reconsider the human rights implications of the powers contained within the Investigatory Powers Act, including a broader focus on the impact of surveillance on a wide variety of human rights, beyond privacy alone;
2. Develop a robust human rights analysis of all surveillance reforms that involves engagement with the public, academics and civil society more broadly;
3. Reaffirm the government’s commitment to strong and robust encryption to ensure digital security, integrity and privacy can be guaranteed through the use of online tools and platforms;
4. Make the right to be free of unwarranted surveillance a cornerstone of surveillance policy and practice;
5. Clearly outline the scope and scale of lawful state surveillance powers to help the public understand what powers can lawfully be deployed;
6. Develop policy to compel private companies to be

We cannot live in a world outside of surveillance, nor can we condemn all forms of surveillance that can be used to keep people safe and improve our online experiences. But we can demand that all powers are properly and robustly regulated to ensure they do not violate our fundamental freedoms, we can call for transparency and openness in the corporate sector, we can get better informed about our rights and responsibilities, and we can deploy PETs to take steps to protect what we can when we use different online services.

Modern digital surveillance is both everywhere and nowhere; it is in how we browse the web, buy things online, communicate with others and complete application forms, but it also forms the bedrock of governments’ approach to counter serious crime and terrorism. It is seldom seen, but the absence of visual confirmation does not mitigate its significance or prevalence. As we continue to produce data through everything we do online, we need to understand how this data generation redefines our sense of self, our protections as outlined in the laws that govern us, and our freedoms to create and express ourselves.
more transparent as to how private data is stored, analysed and shared.

7. Support and fund the delivery of digital literacy and security educational programmes to enable citizens to build their understanding and capacity in relation to ways they can make informed choices as to protecting their digital security and privacy.

8. Improve the processes by which members of the public can play a meaningful role in the legislative process to ensure their concerns are incorporated within all laws drafted and passed in the UK.

Recommendations for private companies
Further to these recommendations, due to the implications of this survey Scottish PEN calls on private companies to:

1. Collect only enough data to ensure users can access the services they choose and be transparent with how it is handled, shared and used;
2. Ensure data is shared in a manner that protects privacy;
3. Ensure all data collected and shared is undertaken with the knowing consent of Internet users;
4. Use plain and straightforward language when outlining privacy and data usage policies to ensure users can understand what they are consenting to;
5. Deploy privacy enhancing technologies in their digital services, including but not limited to encryption and HTTPS by default to ensure their customers and users are protected.

Recommendations for other stakeholders
Here are a few recommendations that fall to civil society organisations but are also relevant to bodies including, but not limited to, educational institutions, libraries, trade unions and technologists.

1. Develop and deliver educational programmes on digital human rights and ways users can protect their rights online;
2. Encourage a multi-disciplinary approach that incorporates a range of viewpoints and expertise to further develop and support public understanding of this complex issue;
3. Interrogate and analyse the deployment of state and corporate surveillance processes and offer necessary support to the public to ensure all developments are understood.

Furthermore, Scottish PEN strongly supports additional research to explore the connection between surveillance and intellectual and creative freedom, particularly the link between surveillance and self-censorship and the impact that growing awareness of new digital surveillance programmes and powers is having on writers and on the universal right to free expression.
Acknowledgements

We would like to thank PEN International for providing funding for interview transcription and research dissemination and PEN America for allowing us to use and modify their original methodology as the basis of this study.

Scottish PEN
Writer’s Museum,
Lady Stairs House,
Edinburgh,
EH1 2PA

info@scottishpen.org
0131 226 5590

This research was supported in part by a grant from PEN International

This work is licensed under the Creative Commons Attribution-Non-Commercial-ShareAlike 4.0 International License. To view a copy of this license, visit www.creativecommons.org/licenses/by-nc-sa/4.0/

Designed by Alexander Mason
Appendix One: Survey Questions

Here is the list of questions we used for the survey sent out to potential participants. They are modified from the original 2013 PEN America study Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor.

1. How closely are you following news stories about government surveillance efforts within the UK?
   a. Very closely
   b. Somewhat closely
   c. Not too closely
   d. Not closely at all
   e. Not sure/Don’t know

2. In general, how worried are you about current levels of government surveillance of Britons?
   a. Very worried
   b. Somewhat worried
   c. Not too worried
   d. Not worried at all
   e. Not sure/Don’t know

3. How concerned are you about each of the following: (Not concerned at all, Not too concerned, Somewhat concerned, Very Concerned, Not sure/not applicable)
   a. Corporations gathering data to track and analyse consumer behaviour and preferences
   b. The UK government secretly accessing journalists’ call records
   c. The UK government’s new law (the Investigatory Powers Act) to collect and analyse data and metadata ((e.g. time and location) on e-mails, browsing and other online activity of Britons)
   d. Suppression of free speech and press freedom in countries other than the UK
   e. Technology companies being compelled to work with the government to provide vast amounts of personal information

4. How close does each of the following come to your own view? (Not close at all, Not too close, Somewhat close, Very close, Not sure/not applicable)
   a. The government’s primary concern is monitoring communication with foreigners – it’s not really interested in domestic surveillance
   b. I have never been as worried about privacy rights and freedom of expression as I am today
   c. Increased government surveillance is especially harmful to writers because it impinges upon the privacy they need to create freely
   d. Most Britons are unconcerned and uninformed about government surveillance
   e. Personal data collected by the government will be vulnerable to abuse for many years because it may never be completely erased or safeguarded
   f. I am worried that a vast amount of data will be in the government hands and vulnerable to bureaucratic bungling, misuse, and partisan abuse
g. Surveillance is something all governments do – there’s really nothing new or worrisome about what’s happening now

h. Widespread data surveillance is an absolutely essential tool for the government in the fight against terrorism

5. Overall, do you approve or disapprove of the government’s collection of Internet data as part of anti-terrorism efforts?
   a. Approve
   b. Disapprove
   c. I am not sure / I don’t know

6. For what reasons, if any, would you consent to increased surveillance on the UK population?
   a. National security & terrorism
   b. Serious crime, such as murder & sexual offences
   c. Copyright infringement
   d. Tackling fraud
   e. For the economic wellbeing of the country
   f. Tackling the illegal trade in people, drugs and other illicit items
   g. For the protection of public health or morals
   h. No reason would be compelling enough
   i. Other (please specify)

7. If you knew that the UK government had collected data about your Internet activity would you feel that your personal privacy had been violated?
   a. Yes, I would feel that my personal privacy had been violated
   b. No, I would not feel that my personal privacy had been violated
   c. I am not sure / I don’t know

8. What government activity might make you use the Internet differently to communicate, research or work? (Click all that apply)
   a. Collection of metadata
   b. Collection of content data
   c. Hacking platforms, networks or devices
   d. Installing backdoors into encrypted platforms
   e. Undermining end-to-end encryption
   f. None of the above
   g. Other (please specify)

9. In what way do you think your behaviour might change?
10. Over the past year or two, have you personally done or seriously considered doing any of the following because you thought your communications might be monitored in some way by the government? (No, I have not; Have seriously considered; Yes, I have; Not sure / Not applicable)
   a. Avoided writing or speaking on a particular topic
   b. Curtailed or avoided activities on social media (e.g. Facebook, Twitter)
   c. Declined opportunities to meet – physically or electronically – people who might be deemed security threats by the UK government
   d. Deliberately steered clear of certain topics in personal phone conversations or e-mail messages
   e. Refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious
   f. Changed or stopped work on specific projects due to increased perception of surveillance
   g. Taken extra precautions to protect the anonymity of sources or others you may have communicated with
   h. Taken extra steps to cover or disguise digital footprints (e.g. used stronger encryption software, changed to more secure digital service provider)

11. Approximately how often do you communicate – by phone, e-mail or other method – with people who live outside of the United Kingdom?
   a. Every day or most days
   b. Weekly
   c. A few times a month
   d. Once a month
   e. Less than once a month
   f. Almost never

12. How old are you?
   a. 18 or under
   b. 19 – 29
   c. 30 – 39
   d. 40 – 49
   e. 50 – 59
   f. 60 – 69
   g. 70 – 79
   h. 80+
13. What is your gender identity?
   a. Female
   b. Male
   c. Transgender (female-to-male)
   d. Transgender (male-to-female)
   e. Non-binary/gender fluid/gender queer
   f. Not sure
   g. Prefer to self-describe (please specify)
   h. Prefer not to say

14. How would you describe your ethnicity?
   a. White - English / Welsh / Scottish / Northern Irish / British
   b. White – Irish
   c. White – Gypsy or Irish Traveller
   d. Any other White background, please describe
   e. White and Black Caribbean
   f. White and Black African
   g. White and Asian
   h. Any other Mixed / Multiple ethnic background, please describe
      i. Indian
      j. Pakistani
      k. Bangladeshi
      l. Chinese
   m. Any other Asian background, please describe
   n. African
   o. Caribbean
   p. Any other Black / African / Caribbean background, please describe
   q. Arab
   r. Any other ethnic group, please describe

15. How would you describe your religion?
   a. Buddhist
   b. Christian (including Church of England, Catholic, Protestant and all other Christian denominations)
   c. Hindu
   d. Jewish
   e. Muslim
   f. Sikh
   g. Any other religion, please describe
   h. No religion
16. If you are a member of Scottish PEN, please identify your affiliation
   a. Writer member
   b. Reader member
   c. Not a member

17. Which of these best described what you do? Check all that apply
   a. Agent
   b. Editor
   c. Educator/Academic
   d. Translator
   e. Writer
   f. Something else (Please specify)

18. If “writer” was one of your responses in the previous question, which of these best describes the type of writer you are? Check all that apply
   a. Academic writer
   b. Biographer
   c. Blogger
   d. Children’s/young adult book writer
   e. Graphic novelist
   f. Historian
   g. Journalist
   h. Memoirist
   i. Narrative non-fiction/essayist
   j. Novelist or short fiction writer
   k. Playwright
   l. Poet
   m. Screenwriter
   n. Something else

19. Would you be willing to participate in a follow-up interview based on your responses to this survey?