

CIS OCCASIONAL PAPER 162

THE CENTRE FOR
INDEPENDENT
STUDIES



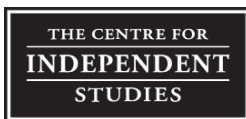
**Liberty and Surveillance:
What should governments
and private corporations
know about you?**

Tom Simpson

Liberty and Surveillance: What should governments and private corporations know about you?

Tom Simpson

CIS Occasional Paper 162



2018

Published January 2018
by The Centre for Independent Studies Limited
Level 1, 131 Macquarie Street, Sydney NSW 2000
Email: cis@cis.org.au
Website: www.cis.org.au

Views expressed in the publications of The Centre for Independent Studies are those of the authors and do not necessarily reflect the views of the Centre's staff, advisers, directors, or officers.

©2018 The Centre for Independent Studies



A catalogue record for this
book is available from the
National Library of Australia

Liberty and Surveillance: What should governments and private corporations know about you?

What I'm here to talk about tonight is the relationship between liberty and security, and where governments should draw the line in terms of what surveillance is permissible. I've got some developed thoughts on that topic which I'll try and share with you, and I would like to move on to think about the role of private corporations in a more speculative vein.

In some ways the surveillance debate has dropped off the agenda. There is plenty of other stuff that people are worried about. In Britain, where I come from, Brexit is dominating the headlines and the rest of the world is trying to make sense of Donald Trump's presidency. So there's plenty of other issues to worry about and legislators have largely made their peace with this issue. But I think there are some deeper themes here which are worth exploring at further length.

Some biography first. I started thinking about this three or four years ago, when one of the UK enquiries in the wake of the Snowden revelations began to look at what the role of Government Communications Headquarters (GCHQ) ought to be. I was invited to contribute to that enquiry and I felt like I ought to have an opinion. I don't know if you sometimes find yourself in that situation. And because of my military background I was expecting

to come to the view that the mass surveillance of the population by the government was probably a necessary and proportionate power which the government needed to have in order to keep the country safe, and that the security services are doing a difficult and usually invisible job with competence and discretion.

Slightly to my own surprise, as I began to think about it, I've come to the view that the issues are more complex, and that mass surveillance is not something that the government should be engaged in. I'm a philosopher by discipline so I have an inbuilt desire to try and get things right. As I'm not a politician I'm also freed from the constraint of worrying about how my words will be received. So I offer what I say here in the spirit of open discussion aimed at getting things right. And I recognise that there are two sides on this. It's a difficult matter of judgement.

So what is 'mass surveillance', this term that I've been using? To give an intuitive way of thinking about it, imagine policing and intelligence work as a fishing task. You're trying to catch the bad folks who are doing bad things. In an analogy, you can either fish with a net or you can fish with a hook. Fishing with a hook is when you're responding to individuals who are doing bad things and you're trying to pull them out and then use the apparatus of the courts and the prison system to make sure that they're not a danger. Fishing with a net is when you're just catching everything that comes along and then out of everything you've caught, you're picking out the things that matter to you.

Intuitively, you can see there is a distinction. It seems to me a characteristic of a free society, that intelligence and policing is done with a hook and not with a net. We do *targeted* surveillance, not *mass* surveillance. If you need to find out about someone who you reasonably suspect of criminal intent, and they're sending letters, then you get the letter off the post line and you steam open that letter. What you don't do is steam open everyone's letters as they come through to find the one that you want.

What Snowden's revelation showed was that the NSA and GCHQ in particular had hacked the internet and were engaged in mass surveillance.

Approximately 85 to 90% of internet traffic goes through the UK and the US. By plugging into the key nodal points for this traffic, the NSA and GCHQ were able to extract that proportion of internet traffic, and they were retaining the content of communications, like telephone calls or emails, for three days.

The communication metadata was retained for 30 days. The reason it was only 30 days is not because of any legislative requirement, but because of capacity. If they could store more they would, was the point. What this allows is network analysis. When you've identified someone of intelligence interest you can then track who they're communicating with, and you can build up an analysis of the terrorist and criminal networks. Obviously the context in a wider sense is 9/11 and Islamist terrorism, and the fast-moving security threats which many countries internationally are facing.

So that's the broad context. The standard argument about the issue then goes like this. Those from a civil liberties perspective say "we have rights to privacy. The state cannot override our rights to privacy without due cause". The claim is then that there is no due cause here which justifies this degree of mass surveillance. That's the starting salvo, if you like, in the debate.

The reply then comes back from the other side, "rights are always *prima facie* only, and they can be overridden when there are competing or more significant rights. And what we face here is a clash of rights. There are rights to privacy, and there are rights to bodily integrity. And the right to bodily integrity — which just means the right not to be attacked, of living without fear — is more significant than the right to privacy, and therefore, the right to privacy is permissibly overridden."

Usually the argument will continue with the claim that the situation has changed since 9/11. "We [the security agencies] tell you that if we didn't engage in surveillance then there would be many more people dying." I don't know what it's like in the Australian context. In the UK about every six months the head of MI5, MI6, or GCHQ, stands up and says, "We foiled ten plots recently." Most of the country believes this information but there's also a portion of the country who thinks, "you're probably exaggerating to justify

your existence and the powers that you have.” There is then an argumentative stasis. If the state is to have secrets then it can't all be publicly disclosed. It must be taken on trust, in a context where trust is lacking.

There is a subtler version of this argument, which defends the state's right to engage in the bulk collection of metadata. Privacy is defined by a community or by a society. Think about the right to information that you or I might have in relation to each other. Suppose, when I walk out of here and walk down the street, you just happen to be going in the same direction as me; there's no right to privacy that's being violated by that. It's public space, it's a public thoroughfare, anyone can go where they want.

When I go through the front door of the hotel, if you follow me in, then while it's still public space of a kind, and there is no privacy violation, there are slightly different norms operating. When I close the door of my hotel room, if you come in through the window, there's definitely a privacy violation. My point is, the norms of where we draw the line between public and private are quite subtle and varied, and different cultures might draw the line in different places.

Accordingly, Mark Zuckerberg, CEO of Facebook, has said that the social norm of privacy has evolved over time. Some say that the 'i-generation' are just relaxed about privacy. I'm already a fuddy-duddy, in my late 30s, and the fact that I'm worried about privacy may say more about me than it does about culture. On this argument, internet communication is more like sending a postcard than it is about sending a letter. If you send a postcard you should expect what you put on there to be read.

These are the two arguments that are normally espoused. I want to question both of them.

The first argument, then. Let me try and depict it in metaphorical terms. We've got certain civil liberties on one side, which protect our individual freedoms to live in particular ways, and the extent of which are directly affected by the security powers that the state enjoys.

And on this other side, we've risk from terrorists and criminals. As the risk increases we need stronger security measures to protect us. This results in the sacrifice of some civil liberties. So we're always

engaged in this process of balancing the security measures that are appropriate for the risk we are exposed to, and therefore adjusting the civil liberties that are possible given that level of risk. As things get worse on the threat side, the security measures become increasingly more invasive.

And at that point I begin to question the metaphor and ask: is there a principled stopping point beyond which we're not prepared to go? Take torture, for instance. Is torture a permissible security measure that we'll introduce in order to confront a particular level of risk? Mass imprisonment without trial? What are the stopping points at which, whatever the rise in risk, we're going to refuse to sacrifice those liberties?

As a military man I understand the pressure to not countenance any stopping point. Certainly torture has in my community previously been an actively considered and quite possibly exercised power, which people thought was necessary to cope with a security threat.

But I'm very hesitant about going there. It seems to me we've got to have some way of saying, "there are some things which we're just not going to do; we're going to have to accept the corresponding rise in insecurity and lives lost as a consequence of not doing this."

So my question is, how do we make sense of this idea that there are some things which we are not prepared to do. The balancing metaphor is a very natural and intuitive way of making sense of what's going on. But what it doesn't capture is the idea that there are some liberties, some freedoms, some ways of living that matter to us, and which we should not be willing to sacrifice even at the expense of a rise of insecurity.

What this prompts is the million dollar question that, when we come to questions, you can ask me and I won't give you an answer. The million dollar question is: how many lives are we as a society prepared to lose, in expectation, in order to protect certain civil liberties? And what are those liberties that we should retain? That's the million dollar question.

Rather than answer this directly, let me explore an alternative way of thinking, which the second argument prompts and which I think says something to this issue. The task is to explain why some

freedoms matter more than others, and why we'll accept risk in other areas in order to retain these freedoms. I propose that a distinctively conservative approach may be of use here. Let me say first what I mean by conservatism in this situation.

Many of you will know Samuel Huntington, of the 'Clash of Civilizations' thesis. He describes conservatism this way. "Conservatism is not just the absence of change. It is the articulate, systemic, theoretical resistance to change." I have come from Oxford, where the refusal to change is, of course, the default assumption for institutional governance. It's not an implication of this form of conservatism that change is never appropriate; in fact, it's a trope of conservative thought that sometimes reform is necessary to preserve what you love. But what could rationally justify such a principled opposition to change?

One reason is found in Edmund Burke. As Burke describes it, government is not an exercise in theoretical abstraction, but 'of practical wisdom which supersedes theoretic science'.

Inherited norms are, in this respect, similar to both the market and democracy. Both the market and the democratic voting systems aggregate private judgments. In the market, the price reflects the aggregate facts of supply and demand, combining private information under conditions of uncertainty. Democracy does something similar in terms of political preferences at a point in time. When they function as they ought to, both market-clearing prices and democratic elections are exercises of the wisdom of the crowd.

Inherited norms play the same role intergenerationally. Norms that we receive from our forebears are judgments about, in particular, the role and proper scope of government. These inherited norms carry the wisdom of prior generations.

In particular, they act as conventions, determining the boundaries between public and private. Prior generations could have drawn the line in different places, but *these* are the lines which in the past have been seen to work. And this is a reply to Mark Zuckerberg's idea that social norms have evolved over time. He's right that they have evolved over time. But it's less clear that he's right that the current direction of travel, whereby increasingly all of life is public, is a socially beneficial one, or inevitable. In fact, I'm a little bit

sceptical about Mark Zuckerberg's judgment on this point, because he personally has benefited very greatly from having changed those norms, namely through privacy by exception and publicity by default. Anti-privacy is Facebook's business model. The question that we now face as a society is: where do we think those norms should be, and do we have reason to change the norms that we have inherited?

Let me give a historical parallel here. The British Postal Service got going during the civil war back in the 1640s and 50s. Cromwell was very effective at using this. There was a central office in London, also where the Spymaster General's department was, run by Samuel Moreland.

The GPO worked overnight, so the post would come into central office at 10pm. The spooks would steam it all open, read everything, reseal it, send it off again. Samuel Moreland defended the practice. "A skilful prince ought to make a watchtower of his general post office and there place such careful sentinels as that by their care and diligence he may have a constant view of all that passes. By the frequent inspection of letters a king soon know the temper of all his principle and active subjects."

Edward Arden was the secretary to the Bishop of Durham. He was personally uninvolved in the lethal politics of the day — I know that politics is getting more contentious but we're not yet killing each other. Long may that continue.

Arden wrote to one of his correspondents that he feared to write much, "for letters are opened and nothing is certain." There's a potential convention here. The convention *could* have settled that anything you send by post was open to public view. It could have been that every letter was just like a postcard, that you should just expect that everything is open to view to everyone all the time.

But there is social value in the convention that did settle, namely that letters are private. For any mode of communication, we face a decision about whether it is public or private. The consequence of deciding that it is public is that the zone of life which individuals and civil society controls, as opposed to the government, diminishes. And insofar as we seek to preserve this mode of communication as one which is private, not public, so we have a principled reason to resist the encroachment of surveillance.

What's really going on here, then, is that what we've got is a boundary line between government and between private individuals and civil society. That boundary has been shifted, initially without due process, and subsequently with legislative approvals. Nonetheless, there has been an expansion of government's reach into our lives, and I suggest that on a conservative way of thinking about things, by which we value the inherited norms, there is reason to be cautious about that, and indeed reason to reject it.

I've lost this argument in the legislatures. Most have come to a different view. The pressing issue which we are going to face over the coming years is the role of private surveillance. What I'm talking about here is surveillance as a business model. The key participants in this market are Google, Facebook, and Amazon, and to some extent Apple. The basic exchange is, we individually give them information and they as companies give us free tailored services and also adverts.

There's just no shortage of stuff to be scared about here. As Eric Schmidt has said — the CEO of Google, so this is from the horse's mouth — “We don't need you to type at all. We know where you've been. We can more or less know what you're thinking about.” And for any of us, if you have a think about the consequences of public revelation of your Google search history and your browsing history, as far as I can see, it's like a secular vision of the last judgment. All your secrets are laid bare for public view.

Obviously enough, there are plenty of people who don't like this. So the debate here is frequently cast as a trade-off of privacy versus efficiency.

But, if you're on the sceptical side — as I think I'm finding myself now — it's much harder to make the argument here. In the public case government makes laws and then does what it wants. Through our voting we can input into the process, but fundamentally it's an exercise of government's coercive power, which it rightly has, but is not something that I as a private individual have any exercise over.

But in the private case, I can choose whether to use Gmail. I can choose whether to go shopping on Amazon. I have consented

to the surveillance. Accordingly, opposition to private surveillance is a far harder case to make. Once I've signed the End User License Agreement I waive my rights to privacy. In the earlier analogy, if I invite you into my hotel room, my rights to privacy are no longer broken. What's not to like about this?

There are two points of contention. I think a shallow response is to question whether informed consent has really been given here. That's a valid concern, but I think it doesn't get to the heart of the issue. A more serious issue is the following. There are plenty of transactions in the marketplace which meet the conditions of consent and which are also, in economic terms, a Pareto improvement – that is, both parties are made better off as a result of that – and in which there is also a proper role for regulation and intervention by government. The obvious example here is monopolies.

All the customers who purchase services or goods from a monopoly do so consensually. They pay the price which shows they think it's worth it for them individually, and obviously the company thinks it's worth it at that price because otherwise they wouldn't be selling it. And yet even with that consent, even with that Pareto improvement, it's still sometimes right that there be controls placed on companies. I think this is the case here too. There are externalities to the transaction which are not captured by the price.

So what are the externalities that arise due to private surveillance? The externalities are colossal asymmetries of bargaining power between these major platforms and consumers and businesses who are selling through them. To make this salient, with an example from 2009: the editor of the Dallas Morning News was in conversation with Amazon to try and get Amazon to host the Dallas Morning News, and make it available on Kindle. He didn't go with the deal, because Amazon wanted a 70/30 split of the subscription revenue. They wanted 70% for providing the distribution service, and were willing to allow 30% for the content providers. That was eight years ago now, and one might expect that Amazon would now be more ambitious on the split.

The externalities we're seeing in these marketplaces are the same as those created by monopolies. There is a loss of consumer choice;

there is excess cost; and most fundamentally, there's agglomerations of money and power. The question is what to do about it, which I will address quickly in closing.

These platforms are natural monopolies in the same way that the rail tracks are a natural monopoly. As there are returns for having one provider of the rail tracks that everyone uses, so there are returns on scale for having centralised platforms which everyone uses to get the relevant service. So the market will always tend towards unification in this context, and this is what gives the internet its winner takes all character. One policy response is to nationalize services that are natural monopolies. I think that that would be a mistake in this context, for all the familiar arguments there. Another response often used by competition policy is to break up monopolies, so that no single provider enjoys monopolistic power. I think that would also be a mistake here, because efficiency for the consumer does depend on there being single operators, and through the economies of scale providing better services than would otherwise be the case. A third model is to recognize the existence of natural monopolies, but to establish regulatory offices who are tasked with ensuring that those corporations do not abuse their power. In the UK, we have regulators for gas and electricity markets, for rail, for communications. These are markets where you want to enable private enterprise to do what it does really well, and also prevent the abuse of monopolistic power that can come with that. It's a tricky line to tread, but important.

Let me sum up. I've been arguing that the standard 'privacy versus security' or 'privacy versus efficiency' debate runs into stasis very quickly. It runs into stasis for quite clear reasons: it fails to articulate a reason for why there would be zones of life which we think ought to be protected, ought to be out of government control or in the private case, ought to be protected from the abuse of corporate power. By thinking about the norms that we have inherited, which demarcate this boundary, and which ensure that valuable ways of living are protected, this explains why we should oppose the handing over of increasing areas of our life to governmental and to private surveillance.



The Centre for Independent Studies is a non-profit, public policy research institute. Its major concern is with the principles and conditions underlying a free and open society. The Centre's activities cover a wide variety of areas dealing broadly with social, economic and foreign policy.

The Centre meets the need for informed debate on issues of importance to a free and democratic society in which individuals and business flourish, unhindered by government intervention. In encouraging competition in ideas, The Centre for Independent Studies carries out an activities programme which includes:

- research
- holding lectures, seminars and policy forums
- publishing books and papers
- issuing a quarterly journal, *POLICY*

For more information about CIS or to become a member, please contact:

Australia

Level 1/131 Macquarie Street,
Sydney NSW 2000 Australia

Ph: +61 2 9438 4377

Fax: +61 2 9439 7310

Email: cis@cis.org.au

www.cis.org.au

Council of Academic Advisers

Professor James Allan
Professor Ray Ball
Professor Jeff Bennett
Professor Geoffrey Brennan
Professor Lauchlan Chipman
Professor Kenneth Clements
Professor Sinclair Davidson
Professor David Emanuel
Professor Ian Harper
Professor Wolfgang Kasper

Professor Chandran Kukathas
Professor Tony Makin
Professor R. R. Officer
Professor Suri Ratnapala
Professor David Robertson
Professor Steven Schwartz
Professor Judith Sloan
Professor Peter Swan AM
Professor Geoffrey de Q. Walker

Liberty and Surveillance: What should governments and private corporations know about you?

Whistleblower Edward Snowden revealed that the NSA hacked the internet as a key part of the 'Five Eyes' intelligence program. Since these revelations in 2013, legislation has largely served to give a secure legal backing to what was previously an undisclosed, covert and sometimes informal national surveillance program. In the private sphere, we are now on the brink of an AI revolution, where machine learning combined with big data will yield unprecedented efficiencies and capabilities.

Privacy and security are both areas of major importance to civil society, so we must ask when does national security surveillance go too far and erode our civil liberties?

Tom Simpson argues that the key issue with both public and private sector surveillance is not a trade-off between privacy and security or privacy and consumer satisfaction. Rather, the key issue is the centralisation of power that big data enables, and the effects that this has on our freedom. The speech also explores ways to make sense of this politically and outline what policy options are available.

Tom Simpson is Associate Professor of Philosophy and Public Policy at the Blavatnik School of Government, University of Oxford, and a Senior Research Fellow at Wadham College. Educated at Cambridge (BA, MPhil, PhD), Tom has previously been a Research Fellow at Sidney Sussex College.

Between degrees, he served as an officer with the Royal Marines Commandos, with tours in Northern Ireland, Iraq and Afghanistan. His research focuses on trust, its theory, practical applications and its implications for both politics and the economy. He is the BBC Radio 3, New Generation Thinker for 2017.



CIS Occasional Paper 162
ISBN 978 1 925744 08 8
ISSN 0155 7386

www.cis.org.au

THE CENTRE FOR
INDEPENDENT
STUDIES