Privacy versus government surveillance: where network effects meet public choice

Ross Anderson

Abstract. The Snowden revelations teach us that many of the world's governments share intelligence behind the scenes. Thirty years ago, a non-aligned country like India could happily buy its military aircraft from Russia; nowadays, although it still buys some planes from Sukhoi, it shares intelligence with the NSA. A rational actor will join the biggest network, and the Russians' network is much smaller. This points us to a deeper truth: that information economics applies to the public sector, just as it applies to private business. The forces that lead to pervasive monopolies in the information industries – network effects, technical lock-in and low marginal costs – are pervasive in the affairs of states too, once we look for them; they are just not yet recognised as such. There are many significant implications, from international relations through energy policy to privacy. Network effects make regulation hard; the USA failed to protect US attorney-client communications from Australian intelligence, just as Australia failed to protect its own citizens' personal health information from the NSA. There are some upsides too; but to identify and exploit them, we need to start thinking in a more grown-up way about what it means to live in a networked world. So, for that matter, must the international relations community.

1. Introduction

The information industries are different; monopolies have been pervasive since the earliest days of computing. First NCR, then IBM, had a near-monopoly of punched-card tabulating equipment; when computing became electronic, IBM translated its dominant position to the new industry, and ruled the roost for years. Computer industry people amassed a lot of empirical experience of what it meant to build, control and exploit a platform; economists also started to study the new industries, and what they learned was systematised and popularised by Shapiro and Varian [1].

There are three reasons monopolies are pervasive in the information industries: network effects, low marginal costs, and technical lock-in. Each of these on its own is familiar from other industries, and each on its own is likely to lead to dominant-firm market structures; when all three are present, there’s an even greater likelihood of a platform race where the winner takes all.

This explains some persistent and formerly puzzling security failures in our industries. For example, computer people had complained for years about the insecurity of leading platforms, such as IBM mainframes in the 1980s, Microsoft Windows in the 1990s, mobile phones in the 2000s and social-network systems now. Information economics explain why security is hard: in platform races, winners are likely to be those who ignored security to make life easy for complementers, such as application developers, and they are then likely to use it to lock customers in later rather than just protecting them from the bad guys [2].

These economic effects do not explain all the dysfunctional aspects of information security nowadays: asymmetric information is pervasive, with consumer security being largely a lemons market, and many cases of moral hazard in systems from payment networks to smart grids. However they are an important part of the explanation. Privacy is harder still: in addition to network effects and asymmetric information, there are many behavioural effects from hyperbolic discounting through user experience to risk salience [3].

However they do help explain many effects beyond mere information security. A further set of examples comes from studying dependability in network industries, from the power industry to the ISPs and other firms that provide the Internet itself [4]. Here again there are other externalities; for example, a utility that suffers an outage faces the cost of lost customer minutes, while the social costs are very much greater. But in many utilities, network effects play a role in industry dynamics, along with technical lock-in and marginal costs.

Curiously, scholars of government appear to have paid little attention to these factors. Experts in public choice study how people act within institutions, while the international relations community observes the interaction between them. The latter school is divided between realists (Thucydides, Machiavelli, Hobbes, Kissinger …) who see relations between states as a cynical zero-sum game, and liberals who believe in international institutions, global norms and interdependence (Kant, Wilson, Keohane, Clinton …) – but even the liberals pay little or no attention to network effects. There is some specialist literature on whether governments should interfere in markets with network effects, or with behaviours that have a social-network component such as smoking and obesity, but this tends to focus on the likely effectiveness of intervention; its takeaway message is the pessimistic one that regulating networked industries is hard, and behaviours with entrenched social-network support can be hard to change.

The Snowden papers reveal an international surveillance network whose scale surprised even industry insiders and security experts. In order to understand how this might be brought under appropriate political, judicial and social control, we need to understand its dynamics. Of course these depend hugely on the economics of the communications service industries; its was the existence of large service firms like Google, Facebook, Yahoo and Microsoft which control the personal information of many millions of people that enabled the intelligence agencies to gain cheap and convenient access via PRISM, while the relatively small number of international cable operators facilitates TEMPORA. But that is not all.

2. Information economics, defence and intelligence

My first big point is that all the three factors which lead to monopoly – network effects, low marginal costs and technical lock-in – are present and growing in the national-intelligence nexus itself. The Snowden papers show that neutrals like Sweden and India are heavily involved in information sharing with the NSA, even though they have tried for years to pretend otherwise. A non-aligned country such as India used to be happy to buy warplanes from Russia; nowadays it still does, but it shares intelligence with the NSA rather then the FSB. If you have a choice of joining a big spy network like America's or a small one like Russia's then it's like choosing whether to write software for the PC or the Mac back in the 1990s. It may be partly an ideological choice, but the economics can often be stronger than the ideology.

Second, modern warfare, like the software industry, has seen the bulk of its costs turn from variable costs into fixed costs. In medieval times, warfare was almost entirely a matter of manpower, and society was organised appropriately; as well as rent or produce, tenants owed their feudal lord forty days' service in peacetime, and sixty days during a war. Barons held their land from the king in return for an oath of fealty, and a duty to provide a certain size of force on demand; priests and scholars paid a tax in lieu of service, so that a mercenary could be hired in their place [5]. But advancing technology brought steady industrialisation. When the UK and the USA attacked Germany in 1944, we did not send millions of men to Europe, as in the first world war, but a combat force of a couple of hundred thousand troops – though with thousands of tanks and backed by larger numbers of men in support roles in tens of thousands of aircraft and ships. Nowadays the transition from labour to capital has gone still further: to kill a foreign leader, we could get a drone fire a missile that costs $30,000. But that's backed by colossal investment – the firms whose data are tapped by PRISM have a combined market capitalisation of over $1 trillion.

Third is the technical lock-in, which operates at a number of levels. First, there are lock-in effects in the underlying industries, where (for example) Cisco dominates the router market: those countries that have tried to build US-free information infrastructures (China) or even just government information infrastructures (Russia, Germany) find it's expensive. China went to the trouble of sponsoring an indigenous vendor, Huawei, but it's unclear how much separation that buys them because of the common code shared by router vendors: a vulnerability discovered in one firm's products may affect another. Thus the UK government lets BT buy Huawei routers for all but its network's most sensitive parts (the backbone and the lawful-intercept functions). Second, technical lock-in affects the equipment used by the intelligence agencies themselves, and is in fact promoted by the agencies via ETSI standards for functions such as lawful intercept.

Just as these three factors led to the IBM network dominating the mainframe age, the Intel / Microsoft network dominating the PC age, and Facebook dominating the social networking scene, so they push strongly towards global surveillance becoming a single connected ecosystem.

The network effects don't just make it difficult for the government of China to separate its infrastructure from the West's; they also entangle developed countries uncomfortably with the surveillance apparatus of rogue states in ways that make it hard to separate 'good' and 'bad' actors. This provides a surprising new twist in international relations. Interesting information has been surfaced by the campaign, led by Privacy International, to ban the export of mass-surveillance equipment to Syria. The Damascus government is using hardware and software supplied by firms in the UK and Germany to watch its population and decide whom to arrest, torture and murder. This has been integrated with more primitive methods, of coercing detainees to hand over social network and email passwords, into an efficient repression machine [6]. Mass-surveillance products should, Privacy International argues, be on the military list and thus covered by sanctions. This was vigorously resisted by GCHQ; if there is some risk that UK troops might end up embroiled in Syria, then the UK government would far rather that the black boxes on Mr Al-Assad's network be supplied from Britain rather than from the Ukraine. But this is embarrassing, given the level and nature of civilian casualties, so the member states of the Wassenaar Arrangement (which sets export control rules) have recently agreed that such

products should require a license [7]. Whether licenses will be granted in secret, or exports continue with an official nod and wink through middlemen in Dubai, remains to be seen.
For present purposes, this example shows that networks are already starting to make international relations more complex. Since their appearance in the nineteenth century, arms export controls have evolved from “don’t sell muskets to the natives” through “sell them just enough missiles that they don’t set up their own factory” to “if they want to monitor and repress their population, we’ll sell them the kit, so we can see what they’re up to.”

My second example of network effects pulling together surveillance systems that used to be separate is the interface between law enforcement and intelligence, which I suspect may be one of the thorniest problems for courts and legislators in the short-to-medium term future.

Historically, the information flow has mostly been from law enforcement to intelligence. One aspect of Snowden’s revelations on which the press has been quiet is the fact that the PRISM system, which caused the initial outcry, is not in fact an NSA system but just an NSA codeword for a data feed managed by the FBI. The large service companies were initially perplexed by the Snowden claims as they did not realise this. They believed they were providing only targeted warranted access to the FBI; it came out only later that an NSA analyst can click on a button on her screen and cause a request to flow automatically through the FBI to their systems. Nothing else could be expected, in countries where the law enforcement agency is considered innocuous.

In the longer term, it may get harder and harder to keep this flow one-way as networks merge, and as the same tools are used by both police and spies. We will return to this question later.

3. Information economics and civil government

Network effects in government are not limited to its defence, intelligence and law enforcement; civil government projects that ignore them risk being ineffective, or failing outright. One example comes from smart meters. The European Union mandated, via the Third Energy Package in 2009, that all Member States introduce smart meters for 80% of their citizens by 2020, subject to an assessment of economic viability, in order to support electricity demand reduction, peak shifting and demand response. However it failed to establish the standards required for smart meters to become a community-wide platform, so countries implementing smart meters are generally using incompatible variants of the technology. This is great for vendors who lock local utilities into expensive meters, but bad for society as the platform is too fragmented to appeal to appliance makers. This also suited the interests of the incumbent energy retailers who want to continue to maximise sales volumes and do not want platforms that could allow market entry by independent energy service companies. As a result, the claims for likely energy savings appear somewhat optimistic [8].

Our second example is intellectual-property law. Lessig has described how a network of international treaty obligations has created an anti-commons that is damaging to industries and cultural traditions which depend on incremental innovation [9]. A security-economics example is the thicket of conflicting patent claims on authentication protocols, one of the two main reasons we’ve been unable to improve browser security and deal with phishing (the other is the network effect created by the two-sided market in servers and clients; no merchant wants to change its web server if it would lose even a few percent of web browsers). The inability of governments to deal with such issues has led to many private initiatives in software licensing, from the FreeBSD license and the General Public License to the Creative Commons.

On a broader canvas, the European Union itself was established and built up to try to enable European industry to compete with US firms; this was seen in the 1960s and 1970s as a matter of market size more than anything else. It started as a customs union and developed into a confederation in which 28 Member States pool sovereignty so as to create a single market. This has not really helped European information industries compete with US ones, as the key factor is not home market size but who gets the global network effects going first and fastest. This is a matter that economists have not studied much; raw material might range from IBM's defeat of ICL in the UK in the 1960s and 70s to the way in which Facebook emerged from among 40+ competing social networks and having defeated Myspace in the US market, picked off the leaders in other national markets one by one.

Even professional politicians are frequently over-optimistic about their own freedom of action as they underestimate the extent of policy lock-in. Recent instances of this range from tussles over the coming referendum on Scottish independence from England, and the Swiss protest vote against EU migrant workers. The latter case illustrates how even a country that is not an EU member state can get into serious difficulties when it passes a law that's incompatible with single-market rules. The EU has emerged as such a strong platform that those neighbouring states which are not members, such as Switzerland, Iceland and Norway, have little choice but to follow most of its regulations – even though they have no MEPs in the European Parliament that makes them. This democratic deficit causes frictions. Should Scotland vote for independence, it would have little choice but to beg for membership on whatever terms it could get; one MEP would be better than none. Politicians find such issues difficult, perplexing and unreasonable; but for IT industry people they are just the world we live in.

We'll return later to the idea of a platform – a trading or other alliance of companies (as with Intel/Microsoft) or nations (as with the EU) which sets the standards, and makes the weather, for a broader ecosystem of actors, whether corporate, state or both; and to the democratic deficit suffered by those actors who are excluded from the table where the deals are done.

So far, so very interesting for the "Foreign Affairs" reader. But what about privacy?

4. Networked states and privacy

The concept of privacy in the English-speaking world has for centuries been tied up with the sanctity of the home as a refuge against the state. In the words of Pitt the Elder

> The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail — its roof may shake — the wind may blow through it — the storm may enter — the rain may enter — but the King of England cannot enter — all his force dares not cross the threshold of the ruined tenement!
>
> *Speech on the Excise Bill,* House of Commons (March 1763).

The sanctity of the home has long been tied up with political rights, and with one's role as a citizen. Until the nineteenth century only home owners and landowners could vote in most UK parliamentary constituencies; and as a labourer in a tied cottage could be evicted if he displeased his employer, home ownership or secure tenancy gave many other less tangible rights as well. The movement to extend the franchise to all male householders, then to all men, and then all adults, operated in parallel with movements for tenants' rights too. In the USA, displeasure with the colonial power's general warrants led to the Fourth Amendment to the Constitution, under which most searches of a home by the police require a warrant based on probable cause.

Technology is challenging this. As a recent report on of the President's Council of Advisers on Science and Technology points out, the proliferation of devices with interfaces based on speech, gesture and video means that there will soon be cameras and microphones in just about every inhabited room of every house [10]. What's more, these devices' dependence on data centres means that law enforcement and intelligence agencies who can serve warrants on these centres (or tap the communications to them) will have access to everything.

How will this be regulated? Well, one of the many shocking things to emerge from the Snowden papers is the way in which the governments of the Five Eyes countries (and beyond) have been prepared to trade their own citizens' privacy for advantage in the network-of-intelligence game. For example, in a meeting about whether Five Eyes states had to minimise metadata revealing sensitive personal information about each others' citizens, only Canada insisted on minimisation. In other words, GCHQ was quite happy for the NSA to know whether a UK citizen like me had ever called a sexual health clinic – and the NSA was quite relaxed about GCHQ having the same information on you. In another case, the NSA was relaxed about its Australian counterpart wiretapping a US law firm that was representing the Government of Indonesia in a case where Australian interests were considered to be at stake. In other words, a foreign intelligence service violated a US law firm's attorney-client privilege, in the USA, using interception facilities largely provided by the US taxpayer. There are several other examples.

Partly this is due to the agencies' traditional focus on 'national security' to the near exclusion of normal civilian considerations, and partly to network effects: players in an intelligence network may come to see their relationship with the other agencies as their key asset, as the one thing that makes them indispensable and enables them to justify the tax money spent on them. (On saying, half-joking, to a senior NSA person that were I Prime Minister I'd abolish GCHQ and leave surveillance to the police, I got a shocked silence followed by "But it's the only way you have of knowing what's going on.") There will always be times when one member state of a network wants to put its own interests first, and again we learn from Snowden that the classified Five Eyes agreement explicitly recognises this. But the net effect is "You can spy on my citizens a bit so long as I can do the same to yours."

So the emerging picture is of rapidly growing cooperation between intelligence agencies on surveillance, with aggressive moves to coerce or co-opt the large service firms who have access to our data, often using law enforcement as a cover. But law enforcement is also pushing for greater cooperation as cybercrime becomes global and the traditional mutual legal assistance treaties turn out to be too slow and cumbersome. The USA encourages this cooperation via the NCFTA, and academics including this writer have encouraged it too [11].

But there is a further factor in play here: the tendency of networks to merge. The Internet itself provides a splendid example; despite much talk of next-generation networks, more-secure networks and low-latency networks for particular applications, in the end everything ends up talking to everything else, and what emerges from that is what we call the Internet. This has caused serious security problems for some industries. An example comes from industrial control systems, which started off running over closed networks and used protocols such as DNP3 that do not support any useful form of authentication or access control. About fifteen years ago, many of these networks suddenly started running over IP, as the technology was becoming universal and was much cheaper. But that meant anyone knowing a sensor's IP address could read it and anyone knowing an actuator's could operate it! This 'oops' moment led to a big push over the past decade to build fancy firewalls to re-perimeterise control networks, with mixed success. However, despite all he scare stories of the Chinese probing our national grids so that they could close off our power supply in times of tension, and despite multiple attempts at regulatory intervention, the move to connect everything up has proved unstoppable.

So: will the intelligence and law-enforcement facilities merge?

In the 'good old days', the signals agency's magic box of tricks was only used for briefing the President or the Prime Minister, and our stolen personal information was so closely held that its theft did us no harm. It was therefore tolerated, even though more and more people started to understand the scope of their operations from the 1970s onwards, thanks to a series of investigative journalists, leakers and historians. But the 'war on terror' let the genie out of the bottle. The UK, for example, has seen two attempts – the Interception Modernisation programme under the last government, and the Communications Data Bill under the present one – which were purported to create a database for police purposes of all the communications data in the UK; not just who called or texted or emailed whom when, but what URLs we visited and the location history of our mobile phones. In each case, the proposed legislation was abandoned after an outcry by the public and in Parliament. Snowden teaches us that the communications database existed all along; in effect, the proposed legislation was a cover under which it could be made available to the police, then the tax inspectors. No doubt the financial regulators will get it next, then the social work department, then the egg marketing board, and finally the dog catcher.

Up till now, the debate on how much the police and other civilian agencies should get has been conducted in rather classical terms. On the one hand, some intelligence veterans claim that giving the police access to their resources will be disastrous, as the tools are just too powerful. Others say that the police can only be given material that won't reveal the limits of government capabilities. On the other hand, managers from other uniformed services such as the customs and the coastguard claim that they get poor wiretap service from GCHQ; how can you justify an expensive capability that's used occasionally to brief the PM when it can be used to save children at risk? If investigations in a networked age will rely on the kind of tools that the NSA, GCHQ and their supplier community have developed, then why should the taxpayer pay for the same development twice?

It looks increasingly like law-enforcement and intelligence systems will merge into a single surveillance system, since the issue engages all of the three reasons that makes information markets different: there are strong network effects, there is technical lock-in growing from the fact that everyone's using the same technology platforms and presenting warrants to the same service firms for the same data; and the back-end systems needed to aggregate, index, and analyse the product have high capital costs and very low marginal ones. Institutional arrangements are starting to reflect this; in addition to the FBI acting as the NSA's funnel into Google and Microsoft, all UK police wiretaps are now done by the National Technical Assistance Centre, which is essentially a service window at GCHQ. There is indeed no point in making the taxpayer buy the same systems twice.

So the next question is whether the systems that actually deliver communications intelligence for national security purposes can be kept separate from, and more capable than, the similar systems used to support law enforcement. Can there be a 'High' service window that lets the spooks do mass surveillance while a 'Low' window lets the cops do the targeted variety? Can the 'High' system alone use cutting-edge collection techniques, so that the 'Low' system will not reveal the limits of national capabilities to (say) a bank inspector or tax collector who might have a foreign lover? In the UK, where wiretapped content is not usable in evidence but the police can get traffic data on demand, perhaps the 'High' window would give content while the 'Low' window gives only metadata. Might that work?

It will be much harder than it looks. For example, it assumes both that intelligence can be kept separate from law enforcement and national agencies from each other. Yet in a post-9/11 world the intelligence task is mostly one of forestalling terrorist attacks – basically a law-enforcement role, and one in which police agencies such as America's FBI and the UK Special branch provide most of the manpower. And most investigations involve more than one country. But the Dutch police make massive use of wiretaps, so if there's good police cooperation, what's to stop an English copper calling in a favour from a buddy in Amsterdam? And how can a political leader justify handing over bulk surveillance data on his entire electorate to foreign intelligence and perhaps police agencies, while denying access to domestic police forces? What happens next time a child is killed in England, and any intelligence officer in the Netherlands or Sweden or Israel could have prevented it? The UK security service already says it might have prevented the terrorist murder of a UK soldier if it had had unrestricted access to the communications of the perpetrators, who used a US communications service provider [12]. The direction of travel is clear. The regulation of surveillance is a going to be a global governance problem, which will be hard to partition along national lines, or into 'intelligence' versus 'law enforcement'.

The privacy of the citizen is just one side of the coin, of course; the other side is the transparency of the ruler. European states link data protection and freedom of information in an attempt to push back on the tendency of information to flow from the weak to the strong. Transparency has clearly increased with search engines and social media and, despite their best efforts, the rulers lose some of their privacy along with their subjects.

What does this mean for privacy lawyers and activists? We'll have to start thinking more about network effects, and how these interact with asymmetric information, agency issues and other effects. We will have to start thinking about the same issues around information monopolies that are tackled by economists advising competition authorities and regulators. If we end up with a world surveillance network, in which all the world's intelligence and law enforcement agencies swap information on all of us as well as buying or coercing it from service companies (who also trade information on all of us), what might an effective regulatory framework look like?

5. A global platform?

Security engineers can suffer from the *déformation professionelle* of seeing only the hazards. Yet we must not forget that the increasingly networked nature of the modern world brings many benefits that also impact on public policy. A networked society is increasingly one in which 'leaders' actually follow rather than lead. For example, if you were to ask a parliamentarian from the outgoing UK government in 2010 what they achieved in three terms in office, you'd have got a long list of reforms from gay marriage to banning smoking in restaurants. Yet these changes happened in pretty well every other European country too over the same period. So where does policy actually come from? The best answer is the billions of interactions we all have every day: the jokes, the calls, the songs, the chats both online and off. Social networks, both physical and electronic, matter too.

What does this mean for international relations? Many realists in the IR community and among commentators in the press and academia take an essentially cyclical view of history. The demise of the US empire is inevitable; but don't worry: so is the demise of the Chinese empire that will follow it. The pessimistic view – used to justify military budgets – is that once an authoritarian country like China surpasses the USA in GDP, and builds more aircraft carriers, then the game is over for civilisation, for democracy and for freedom. Dare we hope that we won't all end up having to learn Mandarin in 20 years' time? (It's not the language of course: it's the fact that China hasn't yet made the democratic transition.)

A networked view of the world is much less fearful, and gives much more emphasis to the liberal view of international relations. 'Civilisation' does not just consist of the USA, plus the Five Eyes allies (or perhaps the NATO allies) simpering at its coat-tails. Civilisation is a network, consisting not just of the citizens and industries of the USA, the EU and the other developed countries, but of the middle classes (for want of a better word) in the less developed countries and in China and Russia too. The US government may occasionally find this annoying – as when a planned takeover of one US firm by another is blocked by the EU's competition authorities despite being approved by the Department of Justice. Yet America should embrace it. Even from a tactical realist perspective, its central position in networks amplifies America's power, an example being the way in which its centrality in payment networks enables it to enforce financial sanctions against states like Iran and North Korea.

From a strategic perspective, the aim should be much higher. The goal of American foreign and defence policy should not be to hang on to its empire as long as possible, but to ensure that America is the last empire. In a rapidly-globalising world, a USA with 300-odd million cannot hope to dominate forever a planet with over a billion Chinese, over a billion Indians, and even 400 million Arabs. The real long-term interest of the USA is to ensure that its empire is replaced by a global network of mutually supporting democracies under the rule of law, rather than by another hegemon.

That may seem a fairly obvious conclusion to an IT industry guy. To a career diplomat, it would mean the victory of liberals over realists. To figure out it would mean in practice – what policies should be pursued by leaders in the USA, Europe and other well-intentioned countries – we need to understand much better how network effects operate within and between governments and the societies they govern. Policy coordination is notoriously hard – ‘like the Loch Ness Monster – much discussed but rarely seen’ [13]; but this too may be an aspect of not understanding and exploiting externalities properly.

6. Conclusion

Power is many things. It’s not just the “hard power” of the number of our aircraft carriers and nuclear warheads, or even the “soft power” of our movie exports and the number of foreign students who come to our universities. It’s our “network power”: the way in which our connectedness enables us to influence others to act as we wish, and to deter them from acting in ways harmful to our interests.

But what does this mean more closely? You might say it’s about influence in an interconnected world, but how do you measure that? A network geek might say it’s about a nation’s centrality in the transactions of interest, but then you have to ask technical questions about what sort of centrality, and whether it’s static or dynamic. Even network researchers don’t really know how to measure network power, and the power elite are at best vaguely aware that it exists. There are perhaps three analogues that politicians may understand: cities, languages and religions. All outlast their founders and some are more governable than others; but the founders’ view of the world can exercise huge influence for generations to come

So this paper is more a statement of an important problem than an attempt at a solution. The message is that it's time that scholars of government to start thinking about information economics. America is, for now, the beneficiary of the same dominant position that makes the big fortunes in the Bay Area; so the US government is in a position to draw on the expertise of business leaders who’ve made their fortunes from understanding network effects, or at least being slightly less slow learners than their competitors. As for the Chinese government, it would be rational to study how information monopolies have been overthrown in the past; the history of Apple may teach at least as much as Sun Tzu or Mao Tse-Tung.

Where does this leave privacy in the age of Snowden? It is very welcome that the NSA review panel recommended that the USA minimise the data it retains on foreigners and restrict the uses that will be made of such data. It is heartening that the administration is thinking about it seriously, and seeking tenders for minimisation software. It is not just an equity issue, as between attack and defence in an agency with both missions. A network view of the world is that such standards, if and when they are embedded in architecture and in policy, are likely become the default surveillance standards for all. What America does to watch users in Britain or Australia or Germany or India will soon be more or less what Britain and Australia and Germany and India do to watch users in America.

If the barriers between nations that participate in the intelligence networks are not sustainable in the long term, and neither are the barriers between intelligence and law enforcement, then what's sauce for the goose will be sauce also for the gander. Policymakers should not delude themselves into believing that a temporary 'home field advantage', as NSA Director General Alexander put it, will last for ever, or even for the lifetime of most of us.

Realising this might lead to a more principled approach to surveillance policy, and one might suggest for example the ethical principles proposed by John Rawls [14]. In it he suggested that the lawgiver act as if behind a veil of ignorance as to what member of society he or she was (or would be reincarnated as); a perspective of fairness can resolve many of the tensions between freedom and equality. Lawmakers should thus perhaps consider what laws they'd make to regulate surveillance if they did not know in what country, or with what social status, they'd be reincarnated. The privacy they grant to a tenant farmer in the Punjab or the Hadhramaut today is likely to be the privacy their children will enjoy tomorrow.

The regulation of surveillance might therefore be a useful early example of what governance could look like in a future networked world, and may in fact be one of the hardest such problems that we face. It contains elements of both fear and hope: fear that an apparatus of global surveillance might be captured by an oppressive successor empire, and hope that there might be no successor, but merely civilisation (whatever that means). This asymmetry may introduce the possibility of new approaches, and nudge realists from selfishness to more enlightened selfishness. As for liberal thinking, the lesson is that we don't just have to rely on international institutions; there are extremely powerful network effects in play, which will be a force for pacification and stability; we must work with them.

In the longer term, the big question is this: what is civilisation, and how do we contribute to its construction? Or to bring it closer to home, what legacy will the USA leave behind when it cedes its leading role in world affairs? Will the world's future networked civilisation be more like a technical network – a platform for rapid innovation but prone to monopolistic abuses? Will it be more like a city, which can be captured by a ruling elite, then flower and decay? Will it be more like a language, which can link a number of polities and allow ideas good and bad to diffuse through them? Or will it be like a religion, a cockpit of struggles for ideological dominance, and vulnerable to violent schism? Quite possibly it will be a mix of all of these. The engineer in me says that the architecture will matter, and the economist says that the incentives will matter too. How we tie the two together could have significant consequences for generations to come. We had better do what we can to ensure that the architecture we create is driven by our hopes rather than our fears, and embodies our deepest values.

Cambridge, England
May 2014

Acknowledgement: I have benefited from helpful discussions of an earlier draft with a number of colleagues: Nick Bohm, Caspar Bowden, Ian Brown, Duncan Campbell, Malcolm Chalmers, Richard Clayton, David Modic, Bruce Schneier, Peter Swire and Sophie van der Zee. I also acknowledge helpful comments from the anonymous referees.

Bibliography

[1] Carl Shapiro and Hal R. Varian, '*Information Rules – A Strategic Guide to the Network Economy*', Harvard Business School Press (1998)

[2] Ross Anderson, 'Why Information Security is Hard –An Economic Perspective', in *Seventeenth Computer Security Applications Conference* (2001), pp 358–365

[3] Michelle Baddeley, 'Information Security: Lessons from Behavioural Economics', *Workshop on the Economics of Information Security,* June 2011

[4] Panagiotis Trimintzios, Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, '*Resilience of the Internet Interconnection Ecosystem*', European Network and Information Security Agency, April 2011

[5] Doris Mary Stenton, '*English Society in the Early Middle Ages*', Pelican 1951

[6] John Scott-Railton, Morgan Marquis-Boire, 'A Call to Harm: New Malware Attacks Target the Syrian Opposition', University of Toronto, 2013

[7] Edin Omanovic, 'The UK & surveillance exports: A piece of CAEC', Privacy International, 10 Jan 2014

[8] Alex Henney, Ross Anderson, `*Smart Meters – Ed Milliband's Poisoned Chalice*', 2012

[9] Lawrence Lessig, '*Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity'* (Penguin Press 2004)

[10] Executive Office of the President of the United States, *'Big Data and Privacy: a Technological Perspective'*, May 2014

[11] Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, *'Security Economics and the Internal Market'*, ENISA 208

[12] David Leppard, 'MI5 spying on internet 'might have saved Lee Rigby'', *The Sunday Times*, 11 May 2014

[13] Olivier Blanchard, Jonathan Ostry, 'The Loch Ness consensus', The Economist, Feb 15 2014

[14] John Rawls, *'A Theory of Justice'*, 1971