Privacy, property and sovereignty in the cyber age

SAMIR SARAN AND ABHIJIT IYER-MITRA

L'affaire Snowden did not tell us anything we did not already know – that governments spy on us. What is new, however, is how heightened perceptions of national security and sophisticated technology are combining to allow these activities by the 'state' to go unnoticed and unchallenged. This paper first examines the three categories of national attitudes that become apparent from the Snowden affair – specifically with regards to privacy and, thereafter, attempts to explain how these attitudes and lack of public awareness are leading to far more dangerous and insidious undercurrents that challenge the foundations of civil liberties, notions of property and definitions of sovereignty as we know them.

All indications are that certain checks and balances were/are being observed – if only on paper – by the United States government in the surveillance of its citizens. No such checks, however, seem to have been applied to foreigners, be they resident in America or their respective countries. What is pertinent, however, is how far America has strayed from its founding principles governing personal freedom and political liberty. It appears that the pendulum has swung so far that the debate is no longer about whether the government should have any right to monitor citizens but rather what the standards and procedures for extraordinary intrusive surveillance should be. The debate in the public sphere has become so securitized that 'national security' is now an open ticket to trample on every right and freedom the US once held sacred. If former President George W. Bush Jr. jeopardized individual liberty with the Patriot Act, President Barack Obama has bestowed on his government the right to be a virtual presence in the lives and bedrooms of billions of people around the world – without care, remorse or debate.

Another disappointment – indicative of this attitudinal shift in America on the subject of privacy – is the stand of the American press on the issue. Far from Snowden's revelations igniting a debate on privacy versus security, the media seems to have bought the security narrative lock, stock and barrel. Evidently the memory of 1971, when Daniel Ellsberg was feted as a hero of liberty by the US media for his leaks exposing 'Vietnam Lies' and forcing a policy reversal on the part of the US government, has long since faded. Every US media outlet has gone to great length to explain the legality and due process of the PRISM spying apparatus and has, almost uniformly, painted Snowden in a poor light.

The second 'state attitude' is that of the EU, where several governments, unlike the US government, led their citizens to believe that they were in fact protected. The EU released its cyber security doctrine earlier this

* This essay draws on two previously published op-ed articles, Samir Saran and Abhijit Iyer-Mitra, 'No to Peeping Sams', *The Hindu*, 18 July 2013 and Samir Saran, 'Keep Cyberspace Free', *Times of India*, 12 September 2013.

year. It repeatedly referred to the EU's core values of freedom of expression and privacy. The document was ostensibly developed around these 'core values'.[1] But this now sounds like a hollow claim, because even as the document was being released, many EU countries were actively colluding with the US and prying into the private lives of their citizens. Unlike the US government which ostensibly protected its own citizens by some form of due process, the European governments allowed blatant violation of their own citizens' privacy. However, most European press outlets, unlike the American media have been savage in their criticism of their own governments; perhaps a more sensitive media ensures the balance of narrative in the EU.

India, however, represents a curious case, unable to secure its citizens either through legislation or by the vigilance of its fourth estate. The country released its National Cyber security Doctrine around the same time that the Snowden issue came into public focus – paying mere lip service to privacy. The word 'privacy' found mention twice in the whole document,[2] appearing as an afterthought. India ostensibly already has a privacy regime that is built into the outsourcing bill, not to protect Indians but to keep the outsourcing industry viable and competitive by promising protection to foreigners and their data. Barely a few weeks after the release of the document, CCTV footage from the Delhi metro of couples getting intimate were found on a pornographic website. No one was held to account, no heads rolled and no apology was forthcoming from any quarter. This episode summarizes India's casual approach to its citizens' privacy – little concern about privacy, on the one hand, and a complete lack of enforcement, on the other.

On the Snowden issue as well, the Indian foreign minister played down reports of US surveillance on Indian citizens, calling it 'cyber-scrutiny', while other members of the government nonchalantly chirped in that 'we too have similar systems in place', as if two wrongs make a right. The Indian media is another story altogether. Far from being a balancer, a competitive hunt for eyeballs has ensured that broadcast and other media are themselves guilty of infringing on private spaces of citizens. Some high profile court cases are in progress and perhaps their outcomes may decide the future of boundaries that the press and media may need to adhere to. The citizen in India in the meanwhile has no respite.

This analysis invariably will lead us to another set of discussions, three among which are perhaps most vital today. The first is that governments, everywhere, snoop and pry on the lives on their own citizens. This is equally true of authoritarian governments like Russia or China, of new democracies like India, securitized democracies like the US, and the 'so called' liberal transparent democracies of Europe that ostensibly do not prioritize security over liberty. Privacy certainly is not a universal or timeless quality.[3] It is defined by who one is talking to, or by the expectations of the larger society in a given context. And, privacy is not the same as security or anonymity. It is the ability to have control over one's definition within an environment that is fully understood. Something, arguably, no one has any more. As Danah Boyd, senior researcher at Microsoft research says, 'Defaults around how we interact have changed. A conversation in the hallway is private by default, public by effort. Online, our interactions become public by default, private by effort.'

The issue is largely one of societal norms complicated by the fact that most personal use is marked by low levels of computational, data and media literacy contributing to heightened fears. This is best exemplified by how different governments and societies reacted to the Snowden revelations. Somehow, there is a misplaced notion that private data and information stored on the cyber cloud is less private than in files in a locker. Possibly this is why breach of privacy in the digital sphere seems more acceptable.

The second issue is that the lack of public (cyber)awareness and literacy is allowing governments to get away with a whole host of actions that would have been unimaginable a decade ago. It is not just dangerous that governments want to police or spy on us; that is something governments have always done. However, until recently such action was more often than not visible; there was a policeman on the road, a camera on the kerb, and so on. But now what is scary is not just the stealth, but that the lack of avenues to challenge and question such surveillance has created a new asymmetry between the government and its subjects. This asymmetry is now redefining privacy norms, property and sovereignty.

The third is that people tend to trust private companies with personal information – usually in blocks – but not governments. Yet, the government,

1. 'Cybersecurity Strategy of the European Union: An Open Safe and Secure Cyberspace', European Union, Brussels, 7 February 2013.

2. 'National Cybersecurity Policy', Ministry of Communications and Information Technology – Department of Electronics and Information Technology, 2 July 2013.

3. Parts of this paragraph have been paraphrased from Q. Hardy, 'Rethinking Privacy in an Era of Big Data', *The New York Times*, 4 June 2012.

with the collusion of private companies, is easily able to triangulate such information to build up a comprehensive picture of individuals. For example ones' Facebook, Twitter and LinkedIn personalities can all be different based on the target audience. Yet the government, with the active collusion of each of these platforms, can build these disparate packets into a comprehensive whole.

In many ways the history of data-mining and the public's acceptance of such data mining for advertising purposes presaged this acceptance of data-mining for security purposes. Data-mining is a complex interdisciplinary operation that involves computers processing vast amounts of information, matching them against preset algorithms, and finding intersections, what are euphemistically referred to as 'points of interest'.[4] In the marketing industry, data-mining helps businesses target individuals for the sale of specific products that they might be interested in. In the domain of security, this becomes the basis for a warrant to allow, for example, a human agent to start scanning personal correspondence. It was in effect the public's acceptance of this in marketing and the private sector that has now exposed them, both practically and normatively, to unprecedented personal surveillance by the government. The private sector has turned out to be the governments' Trojan Horse.

Perhaps the most dangerous outcome of public laxity over data-mining is how legal standards for intrusion have been diluted. Up to a decade back, law enforcement agencies had to painstakingly construct a case of probable cause and present it to the judge. Probable cause is defined as 'information sufficient to warrant a prudent person's belief that the wanted individual had committed a crime (for an arrest warrant) or that evidence of a crime or contraband would be found in a search (for a search warrant).'[5] This then resulted in warrants for further surveillance to acquire information. Today, given that the information available without the warrant is already so vast, that it is not a legal process that is required to gauge intent, but rather a computer code or programme. We are well and truly entering a stage of 'Minority Report' style pre-crime,[6] where mere intent – whether actioned or not, is prosecutable and even worse punishable.

For instance, a husband telling a wife over a casual conversation that 'the president should be shot' would first of all not have been picked up, and second, it would not have been a crime. However, if this same exchange happens over email – not only is it intercepted, but it also falls under a class D felony under United States Code Title 18, Section 871 'Threatening the President of the United States'. So what exactly has changed to merit this conversation to (*a*) being overheard and (*b*) treated as a crime? The latest example of this slippery slope to pre-crime and intent is of the Massachusetts teenager and wannabe rap artist Cameron D'Ambrosio facing 20 years for intent.[7]

This 'intent' is decided again by the data modelling devised by marketing agencies where they targeted a particular customer for a particular product the customer would in fact buy or be very interested in acquiring. While this probabilistic determination is good for 'sales', it cannot be an acceptable basis for conviction and punishment without a date in court. For example – drone strikes can be ordered based on intercepted cyber chatter that determines the so called malafide intent. Such drone strikes effectively blur the line between legally sanctioned pre-emptive actions[8] as opposed to illegal preventative action.[9]

The second Trojan horse is how people's behaviour in the cybersphere has been changing accepted notions of property. The ease of use, and the reach of cyber media, have fundamentally changed both consumer behaviour and created an asymmetric balance of power in favour of the vendor. For example a decade ago, it was possible to buy a book, lend it to friends, photocopy sections of it and more under the fair use exceptions to the copyright act. However, publishing and content houses are today actively underpricing hard copy versions to make soft copies seem attractive, but with overriding controls. For example, most commercial e-books cannot be printed, or even lent to friends. In effect, fair use has been completely removed from the scope without so much as a discussion. The notion of property and right to the property has altered dramatically.

What is happening is the enforcement of commerciality through legislation to force just one kind of transaction which favours the vendor.

4. U. Fayyad, G. Piatetsky-Shapiro and P. Smyth, 'From Data Mining to Knowledge Discovery in Databases', *Artificial Intelligence Magazine*, Fall 1996.

5. *Oxford Companion to American Law*, Oxford University Press, 2002.

6. 'Minority Report' is 2002 blockbuster movie starring Tom Cruise in a future where a special police unit is able to arrest murderers before they commit their crimes.

7. 'Bail denied to Massachusetts teen accused of Facebook terror post', *Reuters*, 25 May 2013.

8. D. Shue and H. Shue, *Preemption: Military Action and Moral Justification*. Oxford University Press, New York, 2007.

9. For an in-depth exploration of the legality of preemption and the illegality of prevention see M. Doyle, *Striking First: Preemption and Prevention in International Conflict*, Princeton University Press, 2008.

Legislation though is not meant to support a commercial transaction, as law has to be neutral between contracting parties. Even the option of differential pricing – where different usages can be bought for different rates – is limited. For example, on the iTunes store, very few songs – priced higher – give one the authority to transfer to another device. Most songs are restricted to the one playback device.

In effect, while benefiting from the unprecedented mass reach of cyber media, content producers are preventing consumers from benefiting similarly from the same. One does not tame the oceans just because one wishes to use the oceans for transport. Rather, the risks are recognized and suitable maritime insurance is procured. Yet, in the cybersphere, instead of dealing with the risks and devising the concept of cyber-insurance, companies are effectively trying to mould this dynamic environment to suit their commercial interests. Our last mile, our user behaviour and our infrastructure is now sought to be regulated, monitored and controlled so as to create 'safe cyber oceans' for the 'virtual ships' to sail on. Private property is now global commons.

This raises several debates about what constitutes property in cyberspace? Contrast the free use exception to copyright laws on hard copies of books described earlier with the case of Megaupload, where the US government insists that since it owns much of the cyber-infrastructure of the world, companies operating outside the US must follow US law. Effectively this is a restating of the 'possession is nine tenths of the law' cliché. On the other hand, it has through legislation stemming from the Trojan horses described earlier, been progressively disenfranchising consumers from claiming similar rights. In fact, not only is property being redescribed, territory and by implication sovereignty itself has acquired a new meaning.

The US has been using cyclic logic to in its attempts at strong-arming to itself cyberspace ownership by mingling civil and criminal complaints and using one to justify the other without proving either. A recent example of such an action by a state on a foreign company is the United States Department of Justice's takedown of the website Megaupload. The site's owner, the now-famous Kim Dotcom, is a resident of New Zealand and a German citizen. Megaupload itself is run out of Hong Kong. So far there does not seem to be any connection to the US. The justification used to go after Megaupload was that the company had leased several servers which were located in Virginia, and was allegedly storing and distributing copyright-infringing files. It has not been proven that any files infringing copyright were being held on the servers in Virginia. Furthermore, Megaupload's users are located throughout the globe, not solely in the United States.

As of now, the rules, which govern the process by which the US serves criminal complaints (the Federal Rules of Criminal Procedure) require an address in the United States where the complaint can be delivered. Despite the fact that the company in question did not have any such address (being registered and run out of Hong Kong), the US was able to proceed. The Justice Department is now recommending that the rules be amended to remove the clause, allowing them to serve complaints on companies with no physical presence in the US. Megaupload's case, United States v Dotcom.

So on one hand while the government is forcing its jurisdiction on cyberspace through claims of physical ownership it, at the behest of the private sector, is denying the same freedom to consumers on their home computers and other media devices. In fact, never before in human history has a corporation enjoyed this much intrusive influence in human lives as the internet has today enabled. And yet, it is the corporation that is sought to be protected.

However, just as private sector data-mining proved to be a Trojan horse to intrusive surveillance, there are signs that such assertion of property laws will at some point undermine the Westphalian concept of a nation state and of sovereignty. Sovereignty has further implications of extra-territoriality which are bound to raise serious hackles in the developing world. For example, in the Megaupload case, US courts are seen demanding that companies which operate in the US must follow US law in their international operations. The argument then is for national sovereignty to be absolute over such infrastructure, where the placing of virtual property in the physical domain of another country necessitates the author of such information to follows the laws of said country. Worryingly, this is a modern example of what European imperial powers did in the 19th and early 20th centuries, imposing their laws, often through coercion, on other nations.

Europe has traditionally been comfortable with notions of extra-territoriality and takes a liberal view of sovereignty. This is evident in its response to the Snowden episode. The European Union (EU) is after all formed on the basis of a slow surrender of sovereignty and most EU states are also members of the North Atlantic Treaty Organization (NATO), allowing US troops stationed there to be governed by US laws. Extra-territori-

ality, therefore, is perfectly legal when it happens with the acquiescence of the host government.

What is surprising though is India's subdued reaction. This is a country that gets riled up by interference in its internal affairs or insults to its sovereignty, perceived or real, owing to its colonial past. Accounts of how the East India Company ended up controlling most of India by acquiring properties through crook and stealth rankle. Yet, in the case of the Snowden revelations, where a foreign government has used stealthy/crooked means to violate Indian laws and penetrate deep into the lives of its citizens, the Indian government has brushed it off. This sets a precedent because, for better or worse, what India has tacitly accepted is US extraterritoriality.

Thoughtless transposition of laws is, however, a recipe for all kinds of disasters. For example, several strategists have argued that much of the tension in the South China Sea is caused by the People's Republic of China extending its understanding of territorial laws based on it being a continental power out to sea. The maritime domain though is a very different beast, requiring very different laws. No analogy is perfect, but this one helps illustrate how concepts imbibed from customary laws in the pre-Internet era are bound to cause significant governance blunders. Now take the accepted paradigm for cyber-sovereignty.

For example, the currently accepted definition is: 'When those infrastructure elements are emplaced within the terrestrial boundaries, territorial waters, or exclusive airspace of a nation-state, it can exert its sovereign authority over them.'[10] However, in light of the Megaupload case, this now seems a patently hollow assertion.

10. A. Casesse, *International Law 81* (2nd edition), 2005.

This reinforces the position that old paradigms that were relevant to the nation state are no longer relevant in cyberspace and as such the issue needs to be dealt with *sui generis*. There is no room for any retrofitting here. And people, communities, states and institutions must begin a new conversation to address these new age posers.

Cyberspace is a free-wheeling mindspace at the cutting edge of innovation precisely because of the absence of sovereignty and artificial barriers. Declaring sovereignty here is as absurd as extending one's jurisdiction deep into the minds of others. One reason for the phenomenal growth of the Internet has been the easy flow of information. In many ways it brings the proven scientific synergies of physical megacities into the virtual world, allowing seamless interaction and massive increases in productivity. If the property and sovereignty debate is not resolved soon, it will result in a fracturing of the cyber-whole, destroying much of what has made the Internet a dynamic force.

There are no solutions that present themselves but certain parting questions are in order: First, can we agree on a common definition of privacy and defaults assumptions on what is private? Can we create private bedrooms and modes for private conversations in the virtual rooms? Second, should commercial interests allow the idea of property to be redefined? Why should the exploitation of the web for business and commerce allow privacy, freedom of expression and property rights to be compromised? And, third, is cyber a 'zero-sum game' and will nations indulge once again in establishing, capturing and redefining sovereign spaces? Or, will this digital age bring an end to the over two centuries of Westphalian existence