GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Slaying the monster

The country reports gathered here have been written at a critical time: new threats of terrorism in countries such as Kenya, the intensification of regional conflicts and wars, the economic isolation of Russia, and a drift towards authoritarianism in many states. Alarming parallels in Japan are made between the rise of totalitarianism ahead of World War II and what is happening now in that country; and there is a sense many have that regional conflicts might spin even more out of control.

At the centre of this is the need for governments to control their futures, and to maintain power over situations that threaten to become ungovernable. One way they do this is through surveillance. This makes these country reports – and the thematic reports that you have just read – highly political. They come in the wake of WikiLeaks revelations, and Edward Snowden's public exposure of United States (US) spying and the so-called "Five Eyes network", linking some of the most powerful countries in a global surveillance programme. They reinforce the idea that human rights are under threat globally.

Common to most of the country reports published here is that states – frequently with the cooperation of business – are acting illegally: their actions are neither in line with national constitutional requirements, nor with a progressive interpretation of global human rights standards. While many profess to be standard bearers of democracy, they are in fact acting illegitimately – they no longer carry the mantle of public good or operate in the best interests of their citizens that have voted them into power. For instance, in South Korea, "Communications surveillance, in particular, which has insufficient legal control given the rapid development of the internet and mobile technologies, has largely extended the power of the police and the intelligence agency beyond the law."

Despite the media attention that Snowden's revelations received, the public at large remains numb to the problems of surveillance, through ignorance, or, in some instances, complicity. In Turkey, "If you do nothing wrong, if you have no illegal business, don't be afraid of wiretapping," a government minister said there.

This attitude of "only bad people should worry" completely misses the point of mass surveillance: it is ubiquitous, widespread, and involves everyone, whether or not you are a "threat to the state", or engaged in criminal activities. This includes legislation allowing authorities to bug an entire room, and capture the conversations of innocent bystanders, or to monitor the public en masse if there is a potential that a suspect happens to be amongst that public.

Moreover, as numerous reports point out, defining who is or is not a "threat to the state" is obviously a slippery concept, and depends on the regime in power, democratically elected or not. Today's friend is tomorrow's enemy. In Pakistan, in the words of the chairperson of Aware Girls:

> I was shocked when I was told that I and my social media communications had been under surveillance for last three years... In my communication with the agencies it was clear that my work for peace and human rights was seen as "anti-state", and I was seen as an enemy rather than an activist.

And for those who imagine a benign government only interested in their welfare, Syria shows how, during a national strike, even the children and families of striking union members were surveilled:

> Firstly, the police acquired all the mobile communication records of union members and their families, including schoolchildren, and tracked the real-time location of their mobile phones – the mobile service providers had offered to provide this at ten-minute intervals for several months.

In fact surveillance can put the security of the average citizen constantly under threat – and can often have even more dire implications for the vulnerable. Without public awareness of this, and transparency in surveillance programmes, a real erosion of human rights occurs.

Sometimes surveillance legislation is rushed through without proper parliamentary discussion, process or media attention. Legislation shifts and

changes, frequently to suit the new needs of the surveillance regime, and only sometimes are there victories for privacy rights, and for transparency – perhaps the most notable being the European Union (EU) cancelling its data retention directive, with a mixed knock-down effect on national legislation amongst EU members.

Argentina shows that even if governments are open about their new programmes to capture and centralise data – in this case biometric data – and emphasise the positive aspects of these programmes, the potential for this to be used in the future in ways that violate the rights of ordinary citizens is extraordinary. Without citizen-driven legislation, and public oversight, democracies are under threat (the story of Frankenstein's monster comes to mind here).

Syria points out that less-democratic states have little impetus to not surveil their citizens. If so-called democracies like the US and the United Kingdom with all their rights and privileges and sturdy legal systems can get away with it, how can we expect struggling democracies not to do the same? Those in totalitarian regimes, the country report argues, suffer a kind of double surveillance, and are subject to the spying by world powers and their own governments: "It is not unrealistic to imagine this to turn into a global overlapping 'spaghetti' of surveillance programmes where everyone is spying on everyone else."

The complicity of business in all of this needs to be directly addressed by civil society. While some service providers seem to be making attempts at transparency by releasing statistics of government requests for information, many – or most – are not. Ostensibly, they feel no obligation to, with human rights not a primary concern. For instance, MTN's involvement in Cameroon requires attention. Beyond service providers and intermediaries – who appear to prefer "business as usual" rather than to rock the boat – the technology companies that make surveillance tools in the first place are a big part of the problem. Obscenely, in Nigeria, there is the allegation that the systems employed there were "tested" on Palestinians.

Marketing data – tracked and acquired without permission from the public – is also a form of surveillance, and one that now involves our children. That this is often done with a smile and a wink by companies who, if they wish, can on-sell data about our daily habits and behaviours as cheaply as mobile phone numbers to whomever – including states, and other business – shows how far business has slipped from anything resembling an interest in consumer rights. Stronger advocacy is needed in this regard, both from consumer rights and human rights groups.

As Senegal points out, it is not only states that do the surveillance. There are numerous cases of companies illegally spying on their employees, whether through monitoring correspondence or even telephonic communications. Surveillance happens in restaurants, nightclubs, outside shops, in cameras mounted on the neighbour's wall – little attention is given to the right to privacy in these instances, or the need to alert the public to the fact that they are being watched.

Secrecy is at the core of surveillance – whether by states or businesses. It is why it works, and why it is a direct threat to our fundamental rights. It is no use to states or to businesses if those being surveilled know about it. To achieve this, new technology needs to be continually developed and sold to governments (and others). Australia argues that Snowden's revelations have resulted in an increased drive towards surveillance, not less: "Since the Snowden leaks, public reporting suggests the level of encryption on the internet has increased substantially. In direct response to these leaks, the technology industry is driving the development of new internet standards."

So how do we slay Frankenstein's monster?

The country reports make several suggestions in this regard. A citizen-driven, balanced approach to legislating surveillance is necessary, with the recognition that some measure of surveillance is in the interests of public safety (against violence and crime, including the protection of children against pornography and child trafficking). Lebanon puts this clearly: "Many argue that online privacy is a human right, while others insist that it is a negotiated contract between the state and its citizens – a contract in which citizens exchange some of their data in return for national security." (Secrecy is, in other words, different to the need for state secrets). Costa Rica argues that citizen oversight in the implementation of national databases and of surveillance programmes is also necessary. Users of the internet can practice safer communications using encryption technology, and other behaviour changes when going online – such as paying more attention to the kind of information they share with businesses or individuals.

The idea of the internet as a free, open space that promotes democracy needs to be revisited. "In mainland China the internet and everything in it can reasonably be viewed as public space – that is, ultimately belonging to the state," the author

contends. In the UK, the Government Communications Headquarters (GCHQ) – the counterpart of the National Security Agency (NSA) in the US – has said: "[W]e are starting to 'master' the Internet… And our current capability is quite impressive… We are in a Golden Age." In this context, as in Switzerland, privacy becomes a "privilege", not a right.

Elsewhere, activists are going "offline" out of necessity and safety. In Indonesia, Papuan activists say: "Now I only trust face-to-face communication. I rarely use the telephone to talk about sensitive issues."

Privacy, transparency and accountability are key words. They are also old struggles. In this sense the terrain has not changed. But these country reports suggest the terrain might just have got rockier, and the path much more perilous.