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

Introduction

Gus Hosein
Executive director, Privacy International
www.privacyinternational.org

The extent to which we communicate is part of what makes us human. The quest to articulate our needs, desires, interests, fears and agonies motivated drawing, the gesture, the spoken word and its written form. Conversations led to letters, couriers led to the post, followed on by telegraphs, telephones, mobiles and internet working. We now relay our most intimate thoughts and interests over communications media. Yet with new revelations and innovations, we are seeing the growing ambitions of governments and companies to track, monitor, analyse and even monetise the communicative actions that are core to our being. To protect human autonomy in modern society, it is essential for us to govern communications surveillance.

Social and technological changes have increased the power and pervasiveness of surveillance. First, nearly everything we do today is a communicative act that is digitally observable, recordable, and most likely logged, and analysed from the earliest of stages, retrospectively, and in real time. Even our movements are logged by service providers.

Second, unlike our ephemeral spoken words amongst friends in a room, nearly every communication can now be collected, analysed, retained and monetised. It is now possible to capture the communications of an entire nation – the modern equivalent of listening to every private and public conversation in rooms, in homes and offices, town halls, public squares, cafés, pubs and restaurants across the nation.

Third, every communication generates increasingly sensitive metadata – data related to the communications – that is captured, logged, rendered accessible, and mined to draw lists of suspects and targets, and to understand our relationships and interactions.

Fourth, nearly every communication today involves a third party – the post office, the mobile phone company, the search engine, and the undersea cable company, who are likely to be tasked with surveillance on behalf of the state.

Fifth, all of this surveillance can now be done in secret – the tampered envelope is now replaced with perfect, secretive replications of communications, captured at a number of points in a network.

Because of these structural changes to communications and the ways we live our lives, there is a new urgency to govern the capabilities of governments to trample on privacy.

- Following us or knowing everywhere we have been is now possible, as our mobile phones routinely connect with nearby mobile phone cell towers. Governments seek to access these logs even as companies seek to data-mine the information for profiling and "big data" analyses.
- Web surfing, the modern equivalent of a walk down the high street and around the public square, is now monitored by analytics companies and, in turn, governments. Both are keen to understand our interests and desires. Consequently, identifying everyone at a public event or in a given area now requires only accessing records from nearby cell towers, or even launching a police-run mobile base station that identifies every proximate mobile device. The powers of "stop and show your papers" will be replaced with the automated and secretive deployment of device scanners.
- While we previously needed secret police and informants to identify people's known associates, governments can routinely generate lists of relationships and track interactions by monitoring our communications metadata from chat, text messaging, social networks, emails, and of course, voice communications. This also helps generate lists of previously unknown suspects or targets. "Guilt by association" could be assessed by who you follow on Twitter, and friends of friends on Facebook.
- And whereas before governments needed to train spies to infiltrate our friendships and other networks, and to search our homes and go through our files, they can merely compromise our computers and mobile phones, surreptitiously turn on our cameras and microphones, and gain access to all our correspondence, documents, images and videos, and even passwords.

Despite all these dramatic changes in capabilities, unprecedented in the history of surveillance and technology, governments are every day seeking to establish new and greater powers, complaining that they are losing capabilities, or "going dark". Yet this is the golden age of surveillance. It is made possible by ambitious intelligence agencies and police services, poorly regulated by politicians who are resistant to understanding technology and human rights. It is spurred by a surveillance industry that develops and sells new technologies to governments across the world. And it is enabled by companies who fail to secure our communications infrastructure, acquiesce to government demands, and do not resist bad policy that make available for access ever larger stores of information on us, generated to profit from our relationships with our friends, families and colleagues.

We must not presume that this is only about communications privacy. As nearly everything involves communication in modern society, communications surveillance can itself generate previously unseen power for the watchers over the watched: individuals, groups and even societies. Because of this, the true debate over surveillance resides in questions of the rule of law: Are some institutions and capabilities above such a totemic principle? When it comes to modern governance, how do our existing governance structures meet the challenges of a new increasingly interconnected society? Or national security: Can effective and identifiable lines be drawn around such an amorphous concept to give clarity to the public?

We have barely scratched the surface on any of these questions, and within all of this we find ourselves racing to the future where the boundaries of privacy will be further tested, innocuous information increasingly revelatory, and the power to surveil increasing in its power and scope.

Nonetheless, I believe that in an open and democratic debate, societies will choose to regulate such power. The challenge is that the debate must be forced upon our governments. Fortunately we now have evidence of some of their secret capabilities, thanks to the incredible contribution from Edward Snowden, and due to investigations into the surveillance industry that markets new capabilities to governments. We must now act upon this knowledge. We must engage with regulators to ensure that they are aware of the weaknesses in their regulated industries.

We must reach out to the legal community so that they understand the risks that surveillance poses to the justice system and the rule of law. We need to work more with technology communities so that they are inspired to build more secure and privacy-enhancing systems. The media and civil society organisations need to be made aware of how surveillance is targeted at journalists and agents of change. We must engage with industry so they understand the dangers of their choices over design of technologies and services and the limited autonomy they provide customers that set new standards for abuse by others. And parliamentarians and policy makers must be informed of the very real roles we expect them to play in the regulation of agencies and the safeguarding of the right to privacy of their citizens. Regulatory structures should never be created to act as false flags of legitimacy: rubber stamps have never been acceptable as a form of regulation, and yet the public is being faced with committees and courts operating in exactly that way.

Ultimately the debate around how to regulate such power requires a public presence within it. Society relies on its members to represent its best interest. The answers to these puzzling and fundamental questions are within us – no one else is going to force the government to understand our needs and expectations other than ourselves. Quite possibly the most important regulatory role lies with the public in guaranteeing that those who watch the watchers know that they are not doing so in isolation. Transparency is a core goal to all of this. Vigilance over the operation of all structures cannot waver: from the intelligence agency in its operations, to the court that authorises its operations, to the committee that oversees the powers and processes to access such power. At the top of this pile is the public: hawkish in its oversight and loud in its judgment.