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

The harms of surveillance to privacy, expression and association

Jillian York
Electronic Frontier Foundation
www.eff.org

Freedom is the freedom to say that two plus two make four. If that is granted, all else follows.

George Orwell, 1984

On 5 June 2013, the *Washington Post* and the *Guardian* simultaneously published documents that would rock the world. The documents, leaked by ex-National Security Agency (NSA) contractor Edward Snowden, were not the first disclosures about the United States' vast surveillance complex, but have arguably had the most impact.

Before last year, awareness of digital surveillance in the US – and indeed, in much of the world – was minimal. Disclosures made by WikiLeaks in 2011 can be credited for an uptick in reporting on surveillance[1] – particularly in the Middle East – but did little to inspire research on the societal impact of it.

The knowledge, or even the *perception,* of being surveilled can have a chilling effect. A 2012 industry study conducted by the World Economic Forum found that in high internet penetration countries, a majority of respondents (50.2%) believe that "the government monitors what people do on the Internet." At the same time, only 50% believe that the internet is a safe place for expressing their opinions, while 60.7% agreed that "people who go online put their privacy at risk."[2]

A member survey conducted by writers' organisation PEN American Center in December 2013 discovered that, since the publication of the first NSA leaks, 28% of respondents have "curtailed or avoided social media activities," while another 24% have "deliberately avoided certain topics in phone or email conversations." Perhaps even more worryingly, a full 16% have avoided writing or speaking on certain topics.[3]

Surveillance affects us in myriad ways. It infringes on our personal freedoms, submits us to state control, and prevents us from progressing as a society.

The equal rights to privacy, speech and association

When we talk about surveillance, it often follows that we speak of the importance of privacy, of being free from observation or disturbance, from public attention. In the US, privacy is a fundamental right, enshrined in the Fourth Amendment to the Constitution.

Of course, this is no coincidence – under King George II, the American colonisers found themselves at the mercy of writs of assistance, court-issued orders that allowed the King's agents to carry out wide-ranging searches of anyone, anytime; a precursor to the modern surveillance state.[4] Once issued, an individual writ would be valid for the King's entire reign, and even up to six months past his death.

It was only after the death of King George II that a legal challenge was mounted. When a customs officer in Boston attempted to secure new writs of assistance, a group of Boston merchants, represented by attorney James Otis, opposed the move. Otis argued that the writs placed "the liberty of every man in the hands of every petty officer," an argument that founding father John Adams later claimed "breathed into this nation the breath of life." It was from this societal shift that the Fourth Amendment was born.

The opposition to surveillance, however, is not borne only out of a desire for privacy. In the United States, the First Amendment – that which

1 CNet. (2011, December 1). Wikileaks disclosure shines light on Big Brother. *CBS News*. www.cbsnews.com/news/wikileaks-disclosure-shines-light-on-big-brother

2 Dutton, W., Law, G., Bolsover, G., & Dutta, S. (2013). *The Internet Trust Bubble: Global Values, Beliefs, and Practices*. Davos: World Economic Forum. www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf

3 The FDR Group. (2013). *Chilling Effects: N.S.A. Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN America. www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

4 Snyder, D. (n/d). *The NSA's "General Warrants": How the Founding Fathers Fought an 18th Century Version of the President's Illegal Domestic Spying*. San Francisco: Electronic Frontier Foundation. https://www.eff.org/files/filenode/att/generalwarrantsmemo.pdf

prohibits the creation of law "respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances"[5] – is often debated, but rarely restricted. It is a set of rights that is paramount in US culture; as Supreme Court Justice Hugo L. Black once stated:

> First in the catalogue of human liberties essential to the life and growth of a government of, for, and by the people are those liberties written into the First Amendment of our Constitution. They are the pillars upon which popular government rests and without which a government of free men cannot survive.[6]

Article 19 of the Universal Declaration of Human Rights similarly provides for the right to freedom of opinion and expression, to "seek, receive and impart information and ideas through any media and regardless of frontiers."[7]

Documents leaked by Edward Snowden in 2013 have demonstrated the extraordinary breadth of the US's and other governments' mass surveillance programmes, programmes which constitute an intrusion into the private lives of individuals all over the world.

The violation of privacy is apparent: indiscriminate, mass surveillance goes against the basic, fundamental right to privacy that our predecessors fought for. The negative effects of surveillance on the fundamental freedoms of expression and association may be less evident in an era of ubiquitous digital connection, but are no less important.

In a 2013 report, Frank La Rue, Special Rapporteur to the United Nations on the promotion and protection of the right to freedom of opinion and expression, discussed the ways in which mass surveillance can harm expression. He wrote:

> Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization.[8]

The harmful effects of surveillance on expression and association are undeniably linked – the right to organise is imperative for political expression and the advancement of ideas. In the US, although the two rights are linked in the First Amendment, historically, they have sometimes been treated separately.

In a landmark 1958 case, *NAACP v. Alabama*, the Supreme Court of the US held that if the state forced the National Association for the Advancement of Colored People (NAACP) to hand over its membership lists, its members' rights to assemble and organise would be violated.[9] This case set the precedent for the Supreme Court's foray into the constitutionally guaranteed right to association after decades of government attempts to shun "disloyal" individuals.

Justice John Marshall Harlan wrote for a unanimous court:

> This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[10]

Today, the data collected by the NSA's various surveillance programmes poses a similar threat to the collection of membership lists. The vast majority of what the NSA collects is *metadata*, an ambiguous term that in this case describes the data surrounding one's communications. That is to say, if the content of one's phone call is the data, the metadata could include the number called, the time of the call, and the location from which the call was made.

The danger in metadata is that it allows the surveiller to map our networks and activities, making us think twice before communicating with a certain group or individual. In a surveillance state, this can have profound implications: Think of Uganda, for example, where a legal crackdown on lesbian, gay, bisexual and transgender (LGBT) activists is currently underway. Under surveillance, a gay youth seeking community or health care faces significant risks just for the simple act of making a phone call or sending an email.

In many countries, there has long been a legal distinction between the content of a message (that is, the message itself), and the "communications

5 U.S. Constitution, Amendment I.

6 Ball, H. (1996). *Hugo L. Black: Cold Steel Warrior.* Oxford: Oxford University Press.

7 Universal Declaration of Human Rights, article 19.

8 United Nations Human Rights Council. (2013) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40. un.org/A/HRC/23/40

9 N.A.A.C.P. v. Alabama. 357 U.S. 449 (1958).

10 Ibid.

data", or metadata. This distinction is based on the traditional model of postal mail, where information written on the outside of an envelope is distinguished from the content of the envelope. This distinction is, however, rendered nearly meaningless by modern surveillance methods, which can capture far more than the destination of a communication, and *en masse*.[11]

In order to argue effectively for and reclaim the right to associate freely without surveillance, it is imperative that such a distinction be made. Digital metadata is different from analogue metadata and its wide-scale capture creates a chilling effect on speech and association. It is time for fresh thinking on the impact of the culture of surveillance on our daily habits.

Changing culture, changing habits

The way that we interact on the internet is undoubtedly changing as a result of our knowledge of mass surveillance. Fortunately, fear and withdrawal are not the only reaction to this knowledge; our habits are changing as well. A September 2013 Pew survey found that 86% of internet users have taken steps to "remove or mask their digital footprints" – steps ranging from clearing cookies to encrypting their email. A further 55% of users have taken steps to avoid observation by *specific* people, organisations, or the government.[12]

Corporations – lambasted for their alleged cooperation with the NSA – are responding to the increased public awareness of mass surveillance as well. In early 2013, before the Snowden revelations, encrypted traffic accounted for 2.29% of all peak hour traffic in North America; now it spans 3.8%. In Europe and Latin America, the increase in encrypted traffic is starker: 1.47% to 6.10% and 1.8 to 10.37%, respectively.[13]

It is also telling that journalism organisations have stepped up in the wake of the Snowden revelations, putting into place systems that will protect future whistleblowers. Jill Abramson, former executive editor of the *New York Times*, stated in 2013 that "[surveillance has] put a chill on really what's a healthy discourse between journalists and our sources, and it's sources who risk going to prison."[14] This realisation has led several publications – including the *Guardian* and the *Washington Post* – to implement a whistleblower platform called SecureDrop, which allows sources to share information with media organisations anonymously and securely.

Similarly, the public discussion around the use of encryption is also growing, as is the funding and development of privacy-enhancing technologies. Governmental and quasi-governmental organisations, such as the US State Department and Broadcasting Board of Governors, as well as non-profits such as the Freedom of the Press Foundation, have increased funding toward tools that can be used to thwart surveillance attempts.

The aforementioned Pew study found that 68% of internet users believe laws are insufficient in protecting their privacy online.[15] Numerous attempts have been made globally to effect change through legal and political channels. The 13 Principles for the Application of Human Rights to Communications Surveillance,[16] developed prior to the Snowden revelations, provides a framework for policy making at the state level. Many of the Principles' 400-plus signatories are utilising the document in their policy advocacy.

As awareness of mass surveillance increases among the populace, it follows that new tactics for opposing it will arise. Given the complex nature of digital spying and the interlinked set of rights it affects, this is imperative. Ending mass surveillance requires consideration not only of its effect on privacy, but its impact on expression and association as well.

11 Electronic Frontier Foundation, Article 19. (2014). *Necessary & Proportionate International Principles on the Application of Human Rights to Communications Surveillance: Background and Supporting International Legal Analysis*. https://necessaryandproportionate.org/files/legalanalysis.pdf

12 Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, Privacy, and Security Online*. Washington, D.C.: Pew Research Center. www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

13 Finley, K. (2014, May 16). Encrypted Web Traffic More Than Doubles After NSA Revelations. *Wired*. www.wired.com/2014/05/sandvine-report/

14 Gold, H., & Byers, D. (2013, October 18) Abramson: 'Nobody won' the shutdown; N.Y. Times: 'Obama emerged the winner'. *Politico*. www.politico.com/blogs/media/2013/10/abramson-nobody-won-the-shutdown-ny-times-obama-emerged-175413.html

15 Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Op. cit.

16 Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India...*(2013, July 10). 13 Principles for the Application of Human Rights to Communications Surveillance*. https://en.necessaryandproportionate.org/text