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

Unmasking the Five Eyes' global surveillance practices[1]

Carly Nyst and Anna Crowe
Privacy International
carly@privacy.org, annac@privacyinternational.org

The revelations of the last year – made possible by NSA-whistleblower Edward Snowden – on the reach and scope of global surveillance practices have prompted a fundamental re-examination of the role of intelligence services in conducting coordinated cross-border surveillance. The Five Eyes alliance – comprised of the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB) – is the continuation of an intelligence partnership formed in the aftermath of the Second World War. The patchwork of secret spying programmes and intelligence-sharing agreements implemented by parties to the Five Eyes arrangement constitutes an integrated global surveillance arrangement that now covers the majority of the world's communications. Operating in the shadows and misleading the public, the Five Eyes agencies boast in secret how they "have adapted in innovative and creative ways that have led some to describe the current day as 'the golden age of SIGINT [signals intelligence]'."[2]

This report summarises the state of understanding about the Five Eyes global domination of communications networks, and explains the most concerning surveillance capabilities developed by the intelligence agencies. It also explores the implications of expanded surveillance powers for the rights to privacy and free expression, and the free flow of information and ideas throughout global communications networks. Finally, it canvasses some of the ways that Privacy International is seeking to unpick the Five Eyes alliance and argues for the restoration of privacy and security in digital communications.

The Five Eyes

Beginning in 1946, an alliance of five countries (the US, the UK, Australia, Canada and New Zealand) developed a series of bilateral agreements over more than a decade that became known as the UKUSA (pronounced yew-kew-zah) agreement. This established the "Five Eyes" alliance for the purpose of sharing intelligence, but primarily signals intelligence (hereafter "SIGINT"). The close relationship between the five states is evidenced by documents recently released by Snowden. Almost all of the documents include the classification "TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL" or "TOP SECRET//COMINT//REL TO USA, FVEY". These classification markings indicate the material is top-secret communications intelligence (aka SIGINT) material that can be released to the US, Australia, Canada, UK and New Zealand. Notably while other alliances and coalitions exist, such as the North Atlantic Treaty Organization, none of the documents that have thus far been made public refer to any of these arrangements, suggesting the Five Eyes alliance is the preeminent SIGINT collection alliance.

The Five Eyes agencies are playing a dirty game. They have found ways to infiltrate all aspects of modern communications networks: forcing companies to hand over their customers' data under secret orders, and secretly tapping fibre optic cables between the same companies' data centres anyway; accessing sensitive financial data through SWIFT, the world's financial messaging system; spending years negotiating an international agreement to regulate access to the data through a democratic and accountable process, and then hacking the networks to get direct access; threatening politicians with trumped-up threats of impending cyber war while conducting intrusion operations that weaken the security of networks globally; and sabotaging encryption standards and standards bodies, thereby undermining the ability of internet users to secure information.

1 This paper is based substantially on "Eyes Wide Open", a report published by Privacy International in November 2013, available at: https://www.privacyinternational.org/reports/eyes-wide-open

2 NSA SIGINT Strategy, 23 February 2012, available at: www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html?ref=politics&gwh=5E154810A5FB56B3E9AF98DF667AE3C8

The Five Eyes is a close-knit group. The level of cooperation under the UKUSA agreement is so complete that "the national product is often indistinguishable."[3] This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means "that SIGINT customers in both capitals seldom know which country generated either the access or the product itself."[4] In addition to fluidly sharing collected SIGINT, it is understood that many intelligence facilities run by the respective Five Eyes countries are jointly operated, even jointly staffed, by members of the intelligence agencies of Five Eyes countries. Each facility collects SIGINT, which can then be shared with the other Five Eyes states.

Code-named programmes that have been revealed to the public over the last decade go some way to illustrating how the Five Eyes alliance collaborates on specific programmes of activity and how information is shared. One important example is the TEMPORA programme, revealed by Snowden. By placing taps at key undersea fibre-optic cable landing stations, the programme is able to intercept a significant portion of the communications that traverse the UK. The *Guardian* has reported that 300 analysts from GCHQ and 250 from the NSA were directly assigned to examine material collected.[5] TEMPORA stores content for three days and metadata for 30 days.

Once content and data are collected, they can be filtered. The precise nature of GCHQ's filters remains secret. Filters could be applied based on type of traffic (e.g. Skype, Facebook, email), origin/destination of traffic, or to conduct basic keyword searches, among many other purposes. Reportedly, approximately 40,000 search terms have been chosen and applied by GCHQ, and another 31,000 by the NSA to information collected via TEMPORA. GCHQ have had staff examining collected material since the project's inception in 2008, with NSA analysts brought to trial runs of the technology in summer 2011. Full access was provided to NSA by autumn 2011. An additional 850,000 NSA employees and US private contractors with top-secret clearance reportedly also have access to GCHQ databases. GCHQ received £100 million (USD 160 million) in secret NSA funding over the last three years to assist in the running of this project.[6]

A core programme that provides filtering capability is known as XKEYSCORE. It has been described by internal NSA presentations as an "analytic framework" which enables a single search to query a "3-day rolling buffer" of "all unfiltered data" stored at 150 global sites on 700 database servers.[7] The NSA XKEYSCORE system has sites that appear in Five Eyes countries.[8] The system indexes email addresses, file names, IP addresses and port numbers, cookies, webmail and chat usernames and buddylists, phone numbers, and metadata from web browsing sessions including searches queried, among many other types of data that flow through their collection points.

While UKUSA is often reported as having created a "no spy pact" between Five Eyes states, there is little in the original declassified documents from the 1940s and 1950s to support such a notion. Crucially, first and foremost, no clause exists that attempts in any form to create such an obligation. As best as can be ascertained, it seems there is no prohibition on intelligence gathering by Five Eyes states with respect to the citizens or residents of other Five Eyes states. There is instead, it seems, a general understanding that citizens will not be directly targeted, and where communications are incidentally intercepted, there will be an effort to minimise the use and analysis thereof by the intercepting state. Outside the Five Eyes, everyone else is fair game, even if they have a separate intelligence-sharing agreement with one or several Five Eyes members.[9]

The rights implications

The world has changed dramatically since the 1940s; then, private documents were stored in filing cabinets under lock and key, and months could pass without one having the need or luxury of making an international phone call. Now, private documents are stored in unknown data centres around the

3 Aldrich, R. (2004). Transatlantic intelligence and security cooperation. *International Affairs*, 80(4), 731-753. www2.warwick.ac.uk/fac/soc/pais/people/aldrich/publications/inta80_4_08_aldrich.pdf

4 Lander, S. (2007). International intelligence cooperation: An inside perspective. *Cambridge Review of International Affairs*, 17(3), p. 487.

5 The Guardian quotes an internal GCHQ report that claims "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures." It was additionally reported that the NSA provided GCHQ with the technology necessary to sift through the material collected.

6 MacAskill, E. (2013, November 2). Portrait of the NSA: no detail too small in quest for total surveillance. *The Guardian*. www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance

7 The Guardian (2013, July 31). XKeyscore presentation from 2008. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

8 Ibid., p. 5.

9 Poitras, L. et al. (2013, July 1). How the NSA targets German and Europe. *Spiegel Online*. www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html

world, international communications are conducted daily, and our lives are lived – ideas exchanged, financial transactions conducted, intimate moments shared – online.

With the advent of the internet and new digital forms of communication, now most digital communications take the fastest and cheapest route to their destination, rather than the most direct. This infrastructure means that the sender has no ability to choose, nor immediate knowledge of, the route that their communication will take. This shift in communications infrastructure means that communications travel through many more countries, are stored in a variety of countries (particularly through the growing popularity of cloud computing) and are thus vulnerable to interception by multiple intelligence agencies. From their bases within the territory of each country, each Five Eyes intelligence agency collects and analyses communications that traverse their territory and beyond.

An analysis of the legal provisions in each of the Five Eyes countries reveals that they fall far short of describing the fluid and integrated intelligence-sharing activities that take place under the ambit of the Five Eyes arrangement with sufficient clarity and detail to ensure that individuals can foresee their application.[10] None of the domestic legal regimes set out the circumstances in which intelligence authorities can obtain, store and transfer nationals' or residents' private communication and other information that are intercepted by another Five Eyes agency, nor the circumstances in which any of the Five Eyes states can request the interception of communications by another party to the alliance. The same applies to obtaining private information such as emails, web histories, etc., held by internet and other telecommunication companies. Carefully constructed legal frameworks provide differing levels of protections for internal versus external communications, or those relating to nationals versus non-nationals.

The Five Eyes agencies are seeking not only to defeat the spirit and purpose of international human rights instruments, they are in direct violation of their obligations under such instruments. The right to privacy is an internationally recognised right.[11] The way the global communications infrastructure is built requires that the right to privacy of communications be exercised globally, as communications can be monitored in a place far from the location of the individual to whom they belong. When an individual sends a letter, email or text message, or makes a phone call, that communication leaves their physical proximity, and travels to its destination. In the course of its transmission the communication may pass through multiple other states and, therefore, multiple jurisdictions. The right to privacy of the communication remains intact, subject only to the permissible limitations set out under human rights law. Accordingly, whenever Five Eyes countries interfere with the communication of an individual, thus infringing upon their privacy, they invoke jurisdiction over that individual, and have to comply with human rights obligations accordingly.

The practice of mass surveillance detailed in the Snowden documents is contrary to international law. The Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, for example, has described the invasiveness of mass interception of fibre-optic cables: "By placing taps on the fibre optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications."[12]

The Special Rapporteur reasons that "[m]ass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception."[13]

Taking action

The intelligence agencies of the Five Eyes countries conduct some of the most important, complex and far-reaching activities of any state agency, and they do so behind the justification of a thicket of convoluted and obfuscated legal and regulatory frameworks. The laws and agreements that make up the Five Eyes arrangement and apply it to domestic contexts lack any semblance of the clarity or accessibility necessary to ensure that the individuals whose rights and interests are affected by them are able to understand their application. Their actions have been justified in secret, on the basis of secret interpretations of international law and classified

10 Privacy International. (2013). *Eyes Wide Open*. https://www.privacyinternational.org/reports/eyes-wide-open

11 Article 17 (1) of the International Covenant on Civil and Political Rights provides: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

12 Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, Frank La Rue, 17 April 2013, A/HRC/23/40, para. 38. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

13 Ibid., para. 62.

agreements. By remaining in the shadows, our intelligence agencies – and the governments who control them – have removed our ability to challenge their actions and their impact upon our human rights. We cannot hold our governments accountable when their actions are obfuscated through secret deals and covert legal frameworks. Secret, convoluted or obfuscated law can never be considered law within a democratic society governed by the rule of law.

We must move towards an understanding of global surveillance practices as fundamentally opposed to the rule of law and to the well-established international human right to privacy. In doing so, we must break down legal frameworks that obscure the activities of the intelligence agencies or that preference the citizens or residents of Five Eyes countries over the global internet population. Trust must be restored, and our intelligence agencies must be brought under the rule of law. Transparency around and accountability for secret agreements is a crucial first step.

Privacy International has spent the last year trying to unpick the Five Eyes alliance. We have sent freedom of information requests to intelligence agencies in each of the five countries, seeking access to the secret agreements that govern the Five Eyes. We have brought legal cases against Britain's GCHQ for mass surveillance and hacking activities, and have sought avenues to take similar complaints in other jurisdictions. We filed a complaint under the OECD Guidelines for Multinational Enterprises against the seven telecommunications companies facilitating UK interception of fibre-optic cables. We have written to the Australian Inspector-General of Intelligence and Security asking her to commence an investigation into the ASD, and to the US Treasury Department and to every data protection authority in Europe seeking an investigation into the SWIFT hacking.

Now we are calling for the UN to appoint a Special Rapporteur on the right to privacy, to ensure that privacy and surveillance issues stay high on the agenda in the Human Rights Council. Support our work here: www.privacyinternational.org.