Losing Our Right to Privacy: How Far is Too Far?

DR MARK S ELLIS*

Introduction

My work commute begins each morning as I leave my flat at number nine Weymouth Street, London. Before exiting the building, my image has been captured by a camera situated in the corridor. As I walk toward Great Portland Street, I pass the first of more than 422,000 London CCTV cameras (about one for every 14 people in the capital). Turning left toward the tube station, I pass another CCTV camera positioned on the corner. Entering Great Portland Street tube station I use my Oyster card to pass through the ticket gateway; the system notes the exact time of my entry. While waiting on the train platform, I notice at least two cameras peering down at the waiting passengers. Inside the train, there are several small cameras strategically positioned to see all the commuters. I exit at Farringdon Station, again using my Oyster card, which registers my location and arrival time. As I walk up Farringdon Street toward my office, I pass two more CCTV cameras. Entering the building where I work, I use my ID badge to activate the elevator and to assure building security personnel that I am, in fact, Mark Ellis.

I retrace the same route on my return home. At no time during this entire journey am I out of view. Whether it is government or private surveillance, I am being watched and followed throughout my commute. Disquieting as this may be, that's not the end of it.

At my office, I receive notice that the Xbox I bought for my son has arrived. I am unaware that the US National Security Agency (NSA), the US Central Intelligence Agency (CIA) and the UK's General

* Executive Director of the International Bar Association, London. I would like to thank Yannic Körtgen for his superb assistance in researching and drafting this article. This article is based on a keynote address given by the author at 'Privacy and Surveillance' (Birkbeck Law Review Conference, London, 31 October 2014).

Communications Headquarters (GCHQ) have been conducting surveillance of many online game networks, including massively multiplayer online role-playing games (MMORPGs) such as World of Warcraft, virtual worlds such as Second Life, and the Xbox gaming console.[1]

I remember that last night I used my credit card online to purchase a plane ticket to the United States. I am oblivious to the fact that my transaction will fall under the purview of a programme called DISHFIRE, a worldwide data collection operation that gathers location data, credit card details, missed call alerts, contact roaming alerts (which indicate border crossings), electronic business cards, credit card payment notifications, travel itinerary alerts, meeting information, text messages, and more.

When I log into my AT&T account, located in the United States, my activity is likely entered into an NSA databank. The NSA is able to turn phone and email logs into sophisticated graphs of social connections that identify a person's associates, their location at various times, their travelling companions, and other personal information.[2]

In a single day in 2012, the NSA collected e-mail address books from over 650.000 accounts. Documents show the Agency collected almost 3 billion pieces of intelligence from US computer networks over a 30 day period ending in March 2013.[3] Furthermore, the NSA collects contacts, on a daily basis, from an estimated 500,000 buddy lists on live-chat services as well as from the inbox displays of web-

[1] Mark Mazzetti, 'Spies Infiltrate a Fantasy Realm of Online Games' *The New York Times* (New York, 9 December 2013) <www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html?pagewanted=all&_r=0> accessed 21 November 2014.

[2] James Risen, 'N.S.A. Gathers Data on Social Connections of U.S. Citizens' *The New York Times* (New York, 28 September 2013) <www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all> accessed 19 November 2014.

[3] Glenn Greenwald, 'Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data' *The Guardian* (London, 11 June 2013) <www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining> accessed 19 November 2014.

based email accounts.[4] Taken together, the data enables the NSA to draw detailed maps of a person's life based on their personal, professional, religious and political connections.

After reviewing my AT&T account emails, I make a call to a work colleague in the United Arab Emirates. I wonder if my call is tracked. In all likelihood, it is.

The NSA has been tracking mobile phone locations around the world by tapping into the cables that connect global networks. The Agency collects more than 5 billion location records daily, enabling analysts to map cell phone owners' relationships by correlating their patterns of movement over time with thousands or millions of other phone users.[5]

The NSA has set up task forces assigned to several smartphone manufacturers and operating systems, including Apple's iPhone and iOS, as well as Google's Android mobile operating system. Similarly, Britain's GCHQ assigned a team to study and crack the BlackBerry.[6]

Under the MYSTIC operation, the NSA has built a surveillance system capable of recording '100 percent' of a foreign country's telephone calls, enabling the Agency to rewind and review conversations as long as a month after they take place.[7]

This is *one* day in my life here in London. I am exposed to a near twenty-four hour surveillance matrix, where my journeys, my

---

[4] ibid.

[5] Barton Gellmann, 'NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show' *The Washington Post* (Washington DC, 4 December 2013) <www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html> accessed 19 November 2014>.

[6] Marcel Rosenbach, 'iSpy: How the NSA Accesses Smartphone Data' *Der Spiegel* (Hamburg, 9 Sepember 2013) <www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html> accessed 14 November 2014.

[7] Barton Gellmann, 'NSA surveillance program reaches "into the past" to retrieve, replay phone calls' *The Washington Post* (Washington DC, 28 March 2014) <www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html> accessed 14 November 2014.

internet transactions and my overseas phone calls can be subject to government monitoring.

Government Surveillance: The Ever Expanding Matrix

The United States and others have defended the collection of vast amounts of phone and internet data with the argument that the mere collection of communications data, even in troves, is not 'surveillance' because it is subject to computerised analysis and a human eye would never look at it.

Theresa May, UK Home Secretary, stated that 'if you are searching for the needle in the haystack, you have to have a haystack in the first place.' She argues, rather arbitrarily, that collecting and storing phone and internet records is not the same as 'mass surveillance' because 'most of the data will not be looked at ... [or] touched.'[8] I find this unsettling, particularly coming from a high ranking government official.

I recognise that surveillance is nothing new, even in liberal countries. However, the dynamic nature of technology has changed both how surveillance can be carried out, and also what can be monitored. The digital age has created new opportunities for communication and information-sharing, and the internet has facilitated the development of large amounts of communications data, or metadata, by and about individuals, including their personal information, their location and online activities, and information about their e-mails and messages.

National legislation and human rights mechanisms have been slow to assess the human rights implications of the digital age on access to communications data. Rights to privacy and freedom of expression, and where to draw the line between what is private and what is public, have yet to be comprehensively considered by human rights bodies.

[8] Brian Wheeler, 'Theresa May: We Need to Collect Communications Data "Haystack"' (*BBC*, 16 October 2014) <www.bbc.com/news/uk-politics-29642607> accessed 14 November 2014.

Our current hyperbolic response grew out of the events of 9/11. Following terrorist attacks on US soil, President George W Bush empowered the NSA and other parts of the US intelligence community to conduct wide-ranging surveillance, dubbed the President's Surveillance Program (PSP), without need of court orders or oversight of any kind.

Between 2004 and 2007, the US Government moved several PSP projects under the authority of the Foreign Intelligence Surveillance Court (FISC), and in 2008 passed the Foreign Intelligence Surveillance Act (FISA) Amendments Act.[9] This led, among other things, to the addition of Section 702 authorising the collection of communications from 'non-US persons' inside the United States for foreign intelligence purposes. In collecting the communications of non-US persons, Section 702 explicitly allowed for the incidental collection of communications by US persons as well.[10]

Post-9/11 legislative initiatives regarding secret surveillance were not only draconian but expansive, reaching far beyond the borders of the US. The repercussions for the international community would be breathtaking.

Revelations by whistleblowers and journalists in 2013 and 2014 suggest that the GCHQ together with other global intelligence agencies are developing and deploying technologies to access global internet traffic, calling records, electronic address books, and volumes of digital communications content.

---

[9] The Foreign Intelligence Surveillance Court (FISC) was established by Congress in 1978 as a special Article III court. It was established as part of Congress' effort to reform America's foreign and domestic intelligence policy in the wake of the Church Commission's report documenting decades of law-enforcement misconduct against domestic civil-liberties groups. As part of this effort, it passed the Foreign Intelligence Surveillance Act (FISA) establishing the FISC and delineating a process for classified judicial review of surveillance for foreign-intelligence purposes.

[10] Ron Wyden, 'Udall, Wyden, Heinrich Urge Solicitor General to Set Record Straight on Misrepresentations to U.S. Supreme Court in Clapper v. Amnesty' (*Ron Wyden: Senator for Oregon*, 21 November 2013) <www.wyden.senate.gov/news/press-releases/udall-wyden-heinrich-urge-solicitor-general-to-set-record-straight-on-misrepresentations-to-us-supreme-court-in-clapper-v-amnesty> accessed 19 November 2014.

The Five Eyes, also known as the FVEY, refers to an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States, all bound by the multilateral UK-USA Agreement to uphold joint cooperation in signals intelligence.[11]

Edward Snowden described the Five Eyes as a 'supra-national intelligence organisation that doesn't answer to the laws of its own countries.'[12] Documents leaked by Snowden in 2013 revealed that the Five Eyes have been intentionally spying on one another's citizens and sharing the collected information with each other in order to circumvent restrictive domestic regulations on spying.[13]

In the months leading up to the Iraq War, the Five Eyes monitored the communications of UN weapons inspector Hans Blix, British agents bugged the office of UN Secretary-General Kofi Annan,[14] and an NSA memo detailed a Five Eyes plan to eavesdrop on UN delegations as part of a 'dirty tricks' campaign to pressure certain countries to vote in favour of using force against Iraq.[15]

This sophisticated surveillance alliance is growing. Denmark, France, the Netherlands, and Norway have joined the Five Eyes to constitute the Nine Eyes.[16] And the most recent Fourteen Eyes construct consists of the Nine Eyes plus Germany, Belgium, Italy, Spain and

---

[11] James Cox, 'Canada and the Five Eyes Intelligence Community' (*CDFAI*, December 2012) <www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf> accessed 14 November 2014.

[12] Tagesschau, 'Interview with Edward Snowden' (*Tagesschau.de*) <www.tagesschau.de/snowden-interview-englisch100.pdf> accessed 19 November 2014.

[13] ibid.

[14] 'UK spied on UN's Kofi Annan' (*BBC*, 26 February 2004) <http://news.bbc.co.uk/1/hi/uk_politics/3488548.stm> accessed 14 November 2014.

[15] Martin Bright, 'Revealed: US Dirty Tricks to Win Vote on Iraq War' *The Guardian* (London, 2 March 2003) <www.theguardian.com/world/2003/mar/02/usa.iraq> accessed 14 November 2014.

[16] Leo Kelion 'NSA-GCHQ Snowden Leaks: A Glossary of the Key Terms' (*BBC*, 28 January 2014) <www.bbc.com/news/technology-25085592> accessed 14 November 2014.

Sweden.[17] According to a document leaked by Snowden, the Fourteen Eyes are officially known as SIGINT Seniors Europe, or SSEUR.[18]

To circumvent domestic surveillance restrictions, states cooperate by exchanging their own surveillance data. For instance, the Federal Intelligence Service (NDB) of Switzerland exchanges information with the NSA. The NSA has been granted access to the Swiss surveillance program Onyx.[19] The *Bundesnachrichtendienst* (BND) of Germany systematically transfers metadata from German intelligence sources to the NSA, having provided the NSA with 500 million records in December 2012 alone.[20] The NSA granted the *Bundesnachrichtendienst* access to X-Keyscore.[21] The *Försvarets radioanstalt* (FRA) of Sweden granted the Five Eyes access to underwater cables in the Baltic Sea.[22] The FRA has been conducting a clandestine surveillance operation targeting the internal politics of Russia on behalf of the NSA, which receives the collected data.[23] In cooperation with the Australian Signals Directorate (ASD/DSD), the Defence Ministry of Singapore and its Security and Intelligence

[17] ibid.

[18] Philip Dorling, 'Singapore, South Korea Revealed as Five Eyes Spying Partners' *The Sydney Morning Herald* (Sydney, 25 November 2013) <www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html> accessed 14 November 2014.

[19] 'NDB und NSA Kooperieren Enger als Bisher Bekannt' *Handelsblatt* (Düsseldorf, 15 September 2013) <www.handelszeitung.ch/politik/ndb-und-nsa-kooperieren-enger-als-bisher-bekannt-496751> accessed 14 November 2014.

[20] 'Überwachung: BND Leitet Massenhaft Metadaten an die NSA Weiter' *Der Spiegel* (Hamburg, 3 August2013) <www.spiegel.de/netzwelt/netzpolitik/bnd-leitet-laut-spiegel-massenhaft-metadaten-an-die-nsa-weiter-a-914682.html> accessed 14 November 2014.

[21] '"Prolific Partner": German Intelligence Used NSA Spy Program' *Der Spiegel* (Hamburg, 20 July 2013) <www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html> accessed 14 November 2014.

[22] 'Sverige Deltog i NSA-övervakning [Sweden Participated in NSA Surveillance]' (*Dagens Nyheter*, 6 September 2013) <www.dn.se/nyheter/sverige/sverige-deltog-i-nsa-overvakning> accessed 14 November 2014.

[23] 'Snowden Files Reveal Swedish-American Surveillance of Russia' (*SVT*, 5 December 2013) <www.svt.se/ug/snowden-files-reveale-swedish-american-surveillance-of-russia> accessed November 14 2014.

Division (SID) have been secretly intercepting much of the fibre optic cable traffic passing through the Asian continent. Such intelligence sharing allows the Five Eyes to maintain a 'stranglehold on communications across the Eastern Hemisphere.'[24]

However, of all of the states participating in this global surveillance framework, the US and the UK stand out in their capabilities and unprecedented deployment of data gathering operations. XKEYSCORE is the international surveillance tool through which NSA analysts search vast databases containing the email, online chats, and browsing histories of millions of individuals around in the world. The XKEYSCORE data has reportedly been shared with other secret services including Australia's Defence Signals Directorate, New Zealand's Government Communications Security Bureau, the British GSCQ, and the German BND.

Data is collected by various means, including upstream tapping, which involves the installation of fibre optic splitters at sites operated by private telecommunications companies; these provide intelligence agencies with a complete copy of all internet traffic across the companies' networks.[25]

Similarly, Britain's global surveillance programme Tempora intercepts the fibre optic cables that form the backbone of the internet. With full knowledge of the companies that own the cables and landing stations, Tempora places intercepts in the UK and overseas.[26]

---

[24] Philip Dorling, 'Australian Spies in Global Deal to Tap Undersea Cables' *The Sydney Morning Herald* (Sydney, 29 August 2013) <www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html> accessed 14 November 2014.

[25] Craig Timberg, 'NSA Slide Shows Surveillance of Undersea Cables' *The Washington Post* (Washington DC, 10 July 2013) <www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html> accessed 14 November 2014.

[26] James Ball, 'Leaked Memos Reveal GCHQ Efforts to Keep Mass Surveillance Secret' *The Guardian* (London, 25 October 2013) <www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden> accessed 14 November 2014.

STATEROOM is a secret signals intelligence collection programme that picks up international radio, telecommunications, and internet traffic. It is operated out of the diplomatic missions of the signatories to the Five Eyes UK-USA Agreement and the members of the ECHELON network.[27]

The NSA PRISM surveillance programme, in cooperation with British intelligence and the *Algemene Inlichtingen en Veiligheidsdienst* (AIVD) of the Netherlands, directly harvests data from the servers of US service providers such as Microsoft, Yahoo!, Google, Facebook, Paltalk, AOL, Skype, YouTube, and Apple Inc.[28]

Under the Royal Concierge surveillance programme, Britain's GCHQ agency uses an automated monitoring system to infiltrate the reservation systems of at least 350 luxury hotels around the world.[29] Other programmes involve the wiretapping of room telephones and fax machines used in targeted hotels as well as the monitoring of computers hooked up to the hotel network.[30]

US and UK authorities do not limit their surveillance to individuals. They aggressively infiltrate technology companies with data centres both in and outside their national borders. For example, the MUSCULAR surveillance program is noted to be 'unusually aggressive' in hacking into Yahoo! and Google data. The programme is operated in the UK, jointly with the GCHQ.[31]

---

[27] Jane Perlez, 'Australia Said to Play Part in N.S.A. Effort' *The New York Times* (New York, 31 October 2013) <www.nytimes.com/2013/11/01/world/asia/australia-participated-in-nsa-program-document-says.html> accessed 14 November 2014.

[28] Barton Gellmann, 'U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program' *The Washington Post* (Washington DC, 7 June 2013) <www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html> accessed 14 November 2014.

[29] Laura Poitras, '"Royal Concierge": GCHQ Monitors Diplomats' Hotel Bookings' *Der Spiegel* (Hamburg, 17 November 2013) <www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html> accessed 14 November 2014.

[30] ibid.

[31] Barton Gellman, 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say' *The Washington Post* (Washington DC, 30

States are accessing communications data at a rapidly growing rate. In the three years that Google has been reporting the requests it receives for communications data, the number has almost doubled, from 12,539 requests in the second half of 2009, to 21,389 in the second half of 2012.[32]

In the UK, as a result of administrative errors, roughly 3,000 innocent people have reportedly been wrongly spied on by law enforcement and other public bodies. People have had their records seized and examined in error, and mistakes in at least 11 cases have led to innocent people being wrongly accused, subjected to house searches, or arrested.[33]

The Times of London recently reported that '[t]ens of thousands of innocent people are having their mobile phones snooped on by police officers using secretive and controversial surveillance technology.'[34] Devices called IMSI Catchers 'intercept and listen to phone calls, collect and read text messages and emails and block phone signals in a specific area.'[35] The deployment of IMSI Catchers 'can be authorised by an officer of chief constable rank without having to seek permission from a judge or government minister.'[36]

The more data is stored, the more governments will collect.

As stated by Alex Spence, '[l]aw enforcement will exploit any database built, if it makes it easier to figure out what the rest of us

---

October 2013) <www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html> accessed 14 November 2014.

[32] Alberto Escudero-Pascual and Gus Hosein, 'Questioning Lawful Access to Traffic Data' (2004) 47(3) Communications of the ACM 77.

[33] Alex Spence, 'Extent of Police "Spying" Exposed' *The Times* (London, 4 October 2014) <www.thetimes.co.uk/tto/news/uk/article4226700.ece> accessed 14 November 2014.

[34] Sean O'Neill, 'Police Sweep Up Phone Data with Secret Snooping Device' *The Times* (London, 1 November 2014) <www.thetimes.co.uk/tto/news/uk/crime/article4254706.ece> accessed 14 November 2014.

[35] ibid.

[36] ibid.

are up to.'[37] As already shown, secret service and law enforcement agencies have extensive means and interest to access data stored by large network providers such as Google. In many cases, agencies can purchase or simply issue their own subpoena (without judicial oversight) and compel companies to turn over sensitive data.[38]

In September 2014, FBI director James Comey lashed out against Apple and Google over plans to provide higher encrypting standards for their smartphones; the FBI claimed that encryption might slow investigations.[39]

Judicial Oversight

The most disturbing and dangerous aspect of this new global surveillance phenomenon is the lack of judicial oversight. Traditionally, surveillance had to be authorised by the judiciary. As technology grows more sophisticated, this safeguard increasingly is weakened or even eliminated.

In the UK, the Secretary of State authorises the interception of communications.[40] It is more than a little ironic that the UK employs the same oversight mechanism as the dictatorial government in Zimbabwe where such authorisation comes from the Minister for Transport and Communication.[41]

In the UK, where law enforcement authorities are empowered to authorise their own requests for communications information, approximately 500,000 such requests are reported every year.[42] The Regulation of Investigatory Powers Act 2000 (RIPA), allows

[37] Spence (n 33).

[38] ibid.

[39] RT, 'FBI Director Lashes Out at Apple, Google for Encrypting Smartphones' (*RT*, 26 September 2014) <http://rt.com/usa/190980-comey-fbi-encryption-phones> accessed 14 November 2014.

[40] Regulation of Investigatory Powers Act 2000, section 5.

[41] Interception of Communications Act 2006, section 5.

[42] 'Google Transparency Report' (*Google*, 2013) <www.google.com/transparencyreport/userdatarequests> accessed 14 November 2014.

authorities to obtain communications records without permission from a judge.

Recently, Foreign Secretary Philip Hammond rejected the idea that 'judges should approve electronic surveillance warrants, and claimed that only ministers could exercise the political judgement required to ensure that such surveillance was necessary and proportionate.'[43] This is an extraordinary statement and directly contradicts a fundamental principle of the rule of law, namely that judicial oversight is required to protect against intrusive government policies.

In the same vein, it is highly questionable whether mass surveillance operations in the US are reviewed by 'competent' judicial authorities. There are serious concerns about whether the FISC has a sufficient understanding of the technologies used, or sufficient resources to conduct the oversight required of it.

The Chief Judge of the FISC, Judge Walton, has recognised that the Court is limited in its ability to scrutinise NSA abuses: 'The FISC is forced to rely upon the accuracy of the information that is provided to the Court … The FISC does not have the capacity to investigate issues of noncompliance.'[44] Because it lacks technical expertise in anti-terrorism, the FISC is often forced to defer to NSA judgments. As recently revealed, 'the FISC has denied not a single surveillance request in the past three years. By any measure, the court is simply a rubber stamp for the executive branch.'[45]

The FISC includes 11 US district court judges from at least seven judicial circuits. The Supreme Court Chief Justice selects all judges.[46]

---

[43] Julian Borger, 'Ministers Should Assess UK Surveillance Warrants, Says Philip Hammond' *The Guardian* (23 October 2014) <www.theguardian.com/uk-news/2014/oct/23/uk-gchq-electronic-surveillance-warrants-philip-hammond-mi6> accessed 14 November 2014.

[44] Carol Leonnig, 'Court: Ability to Police U.S. Spying Program Limited' *The Washington Post* (Washington DC, 15 August 2013) <www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html> accessed 14 November 2014.

[45] Christopher Sprigman and Jennifer Granick, 'The Secret FISA Court Must Go' (*The Daily Beast*, 24 July 2013) <www.thedailybeast.com/articles/2013/07/24/the-secret-fisa-court-must-go.html> accessed 14 November 2014.

[46] 50 USC § 1803(a)(1).

Every FISC judge currently serving was appointed by current Chief Justice John Roberts, who was himself appointed by President George W Bush. Roberts' nominations to the FISA court are almost exclusively Republican, with only one judge being a Democrat.[47] FISC judges do not require confirmation by Congress.[48]

The Court sits *ex parte*. Only the judges and government officials are present during the hearings, and only government attorneys can file applications with the Court.[49] Hearings 'must be conducted within the Court's secure facility.'[50] *Ex parte* proceedings are at odds with basic norms of due process such as the right to notice, the right to a public hearing, and the right to confront adversaries.[51]

On rare occasions, the Court will receive an adversarial briefing, usually in the context of the Freedom of Information Act or First Amendment rights. However, the 'FISA does not provide a mechanism for the Court to invite the views of nongovernmental parties.'[52]

Moreover, because FISC rulings are secret, with no public access to the opinions that set precedent, the FISC is effectively 'creating a

[47] Ezra Klein , 'Did You Know John Roberts Is Also Chief Justice Of The NSA's Surveillance State?' *Washington Post* (Washington DC, 5 July 2013) <www.washingtonpost.com/blogs/wonkblog/wp/2013/07/05/did-you-know-john-roberts-is-also-chief-justice-of-the-nsas-surveillance-state> accessed November 14 2014.

[48] ibid.

[49] See USFISC Rules of Proceeding R 6.

[50] ibid at R 17(b).

[51] Conor Clarke, 'Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate' (2014) 66 Stan L Rev Online 125 (2014) <www.stanfordlawreview.org/online/foreign-intelligence-surveillance-court-really-rubber-stamp-ex-parte-proceedings-and-fisc-win> accessed 19 November 2014.

[52] Letter from Reggie B Walton, Presiding Judge of the US Foreign Intelligence Surveillance Court, to Senator Charles E Grassley, Ranking Member of the Senate Committee on the Judiciary (29 July 2013) 7 <www.fas.org/irp/news/2013/07/fisc-leahy.pdf> accessed 19 November 2014.

body of secret law.'[53] Rulings are classified and rarely released.[54] The Court simply does not operate with procedural or legal transparency.

This, together with the FISC's alarming 99.97% approval rate for surveillance requests, has led critics to label the Court a mere 'rubber stamp' for the executive branch.[55]

The FISC has been compared to the English Star Chamber. Legal scholar Randy Barnett stated '[s]ecret judicial proceedings adjudicating the rights of private parties, without any ability to participate or even read the legal opinions of the judges, is the antithesis of the due process of law.'[56]

The lack of judicial oversight extends even further. Many NSA surveillance programmes are not subject to *any* external oversight. Even programmes subject to congressional and judicial review lack real transparency and accountability.[57] Although the programmes

---

[53] Kathleen McCarthy, 'Government Secrecy Threatens America's Rule of Law' (*River Cities Reader*, 30 October 2013) <www.rcreader.com/commentary/secrecy-threatens-rule-of-law> accessed 21 November 2014.

[54] Ben O'Neil, 'FISA, the NSA, and America's Secret Court System' (*Mises Institute*, 22 February 2014) <http://mises.org/daily/6672/FISA-the-NSA-and-Americas-Secret-Court-System> accessed 19 November 2014.

[55] E.g. 'Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S Comm on the Judiciary' 113th Cong 49 (2013) (statement of Professor Laura K Donohue, Georgetown University Law Center) <http://scholarship.law.georgetown.edu/cong/117>; Theodore W Ruger, 'Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective' (2007) 101 Nw U L Rev 239, 245; Spencer Ackerman 'FISA Chief Judge Defends Integrity of Court over Verizon Records Collection' *The Guardian* (London, 6 June 2013) <www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance>; Carol D Leonnig and others, 'Secret-Court Judges Upset at Portrayal of "Collaboration" with Government' *Washington Post* (Washington DC, 29 June 2013) <www.washingtonpost.com/politics/secret-court-judges-upset-at-portrayal-of-collaboration-with-government/2013/06/29/ed73fb68-e01b-11e2-b94a-452948b95ca8_story.html> all accessed 19 November 2014.

[56] Ben O'Neil, 'FISA, the NSA, and America's Secret Court System' *Mises Institute* (22 February 2014) <http://mises.org/daily/6672/FISA-the-NSA-and-Americas-Secret-Court-System> accessed 19 November 2014.

[57] Cindy Cohn and Mark M Jaycox, 'NSA Spying: The Three Pillars of Government Trust Have Fallen' (*Electronic Frontier Foundation*, 15 August 2013) <www.eff.org/deeplinks/2013/08/nsa-spying-three-pillars-government-trust-have-fallen> accessed 19 November 2014.

run under the FISA are subject to FISC review, there is no oversight provided by an external entity. As adroitly described by Mark Rumold, '[t]his secret court isn't in a developing nation, struggling beneath a dictatorship. It's not in a country experimenting for the first time with a judiciary and the rule of law. … No, the court is here, in the United States (it's in Washington, D.C., in fact).'[58]

In one more twist, the Senate Intelligence Committee, which provides congressional oversight of the NSA, relies on information provided by the NSA.[59]

There is a staggering lack of due process in government surveillance programmes. Individuals under scrutiny receive no notice nor have opportunities to contest. Telecommunications service providers who receive demands for records are generally prevented from notifying anyone about the demands. With few exceptions, operations are conducted secretly and individuals are never notified that the NSA or other agencies are collecting their data.

International Legal Protection

International human rights law provides useful, though rarely followed, guideposts for surveillance programmes. Both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) provide that 'no one shall be subjected to arbitrary interference with his privacy ... and that everyone has the right to the protection of the law against such interference or attacks.'[60]

---

[58] Mark Rumold, 'EFF Takes FOIA Fight Over Secret Wiretaps to the Foreign Intelligence Surveillance Court' (*Electronic Frontier Foundation*, 22 May 2013) <www.eff.org/deeplinks/2013/05/EFF-takes-fight-against-secret-law-to-FISC> accessed 19 November.

[59] Trevor Timm, 'A Guide to the Deceptions, Misinformation, and Word Games Officials Use to Mislead the Public About NSA Surveillance' (*Electronic Frontier Foundation,* 14 Aug 2013) <www.eff.org/deeplinks/2013/08/guide-deceptions-word-games-obfuscations-officials-use-mislead-public-about-nsa> accessed 19 November 2014.

[60] Article 12 of UDHR and Article 17 of the ICCPR.

In its general comment, the Human Rights Committee emphasised that compliance with Article 17 of the ICCPR required that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*. 'Correspondence should be delivered to the addressee without interception and without being opened or otherwise read.'[61]

The right to privacy is also protected in various other international and regional human rights legislation.[62]

Recently, scholars have asserted that human rights law, including the ICCPR, either does or should give foreign nationals abroad rights against US surveillance.[63]

Under international human rights law, interfering with the right to privacy is only permissible when it is neither arbitrary nor unlawful. The Human Rights Committee has stated that the term 'unlawful' implies that no interference can take place 'except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.'[64]

---

[61] Official Records of the General Assembly, 43rd Session, Supp No 40 (A/43/40) annex VI [8].

[62] United Nations Convention on Migrant Workers, Article 14; UN Convention of the Protection of the Child, Article 16; International Covenant on Civil and Political Rights; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child; Article 11 of the American Convention on Human Rights; Article 4 of the African Union Principles on Freedom of Expression; Article 5 of the American Declaration of the Rights and Duties of Man; Article 21 of the Arab Charter on Human Rights; and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security; Free Expression and Access to Information; Camden Principles on Freedom of Expression and Equality.

[63] Marko Milanovic, 'Foreign Surveillance and Human Rights' (*EJIL: TALK!*, 27 November 2013) <www.ejiltalk.org/foreign-surveillance-and-human-rights-part-3-models-of-extraterritorial-application>; cf. David Cole, 'We Are All Foreigners: NSA Spying and the Rights of Others' (*Just Security*, 29 October 2013) <http://justsecurity.org/2013/10/29/foreigners-nsa-spying-rights>; Jennifer Granick, 'Foreigners and the Review Group Report: Part 2' (*Just Security*, 19 December 2013) <http://justsecurity.org/2013/12/19/foreigners-review-group-report-part-2> all accessed 19 November 2014.

[64] Official Records of the General Assembly (n 61) [3].

The Committee explained that the introduction of this concept 'is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.'[65] Thus, 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.'[66]

The bottom line is that global surveillance programmes regularly fail to meet these requirements.

Furthermore, under the legality principle, any limitation to the right to privacy must be prescribed by law. A state must not adopt or implement any measure that interferes with the right to privacy in the absence of an existing publicly reviewable legislative act, sufficient to ensure that individuals have advance notice of and can foresee its application.[67]

Yet almost without exception, government surveillance programmes are conducted in secret and are largely governed by a body of secret law developed by a government entity or court which selectively interprets the law.

At least in Europe we are beginning to see some pushback by judicial bodies. The European Court of Justice recently ruled that comprehensive data retention, being disproportionate to the ends sought, interferes with privacy rights and the protection of personal data under the EU Charter of Fundamental Rights; it thus struck down EU Directive 2006/24/EC on data retention.[68] However, the UK seems to be ignoring, or aggressively circumventing the Court's ruling. Newly enacted legislation still grants British intelligence and law enforcement agencies access to millions of people's communications[69] and does not adequately address the human rights

[65] ibid para 4.

[66] Communication No 488/1992, *Toonan v Australia*, [8.3]; see also Communications Nos 903/1999, [7.3] and 1482/2006 [10.1] and [10.2].

[67] For example *The Sunday Times v The United Kingdom* (1979) Series A no 30 [49].

[68] Joined Cases C-293/12 *Digital Rights Ireland v Minister for Communications* and C-594/12 *Kärntner Landesregierung* (OJ C 175/6, 8 April 2014).

[69] Data Retention and Investigatory Powers Bill (DRIP) 2014.

requirements set out by the Court; it actually expands government surveillance powers further.[70]

Conclusion

With national security threats coming increasingly from clandestine groups, surveillance operations have shifted from observing foreign state activity to observing populations. Shortly after the NSA programme was revealed, a US poll showed that a majority of respondents (56%) thought it acceptable if their phone calls were monitored. Clearly, public perceptions of surveillance are shifting. In many ways, our high tech surveillance culture is also a product of modernity; as people grow accustomed to the technology, they are less likely to perceive it as an intrusion into privacy.

This is a worrisome trend. I recall as a 7th grader in 1970 reading George Orwell's book *1984*. I was deeply moved and troubled by this fictionalised account of a surveillance society. If someone had asked me back then if I could imagine the kind of surveillance I have described in this article, I would have rejected the possibility as improbable and unacceptable. Yet, governments have engaged in systematic fear mongering and efforts to create an environment of constantly heightened security. States have changed the very lexicon of security and surveillance. If we accept this shift today, what will be acceptable thirty years from now? How far is too far?

[70] ibid. DRIP does not only ignore the main parts of the ECJ ruling but also amends the initial Regulation of Investigatory Powers Act 2000 (RIPA). Clauses 3 to 5 of the Bill extend both the territorial scope of RIPA and the definition of 'telecommunications service' within RIPA to include webmail services. See Pam Cowburn, 'DRIP: Five Arguments Against Proposed UK Data Retention Bill' (*Media Policy Project Blog*, 15 July 2014) <http://blogs.lse.ac.uk/mediapolicyproject/2014/07/15/drip-five-arguments-against-proposed-uk-data-retention-bill> accessed 19 November 2014.