Tapping the Tubes: Understanding the Geography of Data

https://www.e-ir.info/2013/08/25/tapping-the-tubes-understanding-the-geography-of-data/

HENRY PHILIPPENS, AUG 25 2013

The revelations made by whistle-blower Edward Snowden over the course of the summer of 2013 have taken the world by storm. The two major themes in this saga surprised the general public, officials and politicians alike. Firstly, the size and the extent of the alleged American, British (and later French) data-trawling practices were met with shock. Secondly, the alleged eavesdropping by the US on the European Union and on a number of European allies was equally met with consternation. Yet, as noted by a number of analysts and serving and former politicians, these practices are neither entirely new nor unique.[1] Those familiar with the previous disclosures of information-gathering programs can see the evolutionary progression from older initiatives.[2] Moreover, all governments conduct espionage, to the best of their abilities, whether for political, security, economic or technological purposes.[3]

However, in an age characterized by electronic communications, big data and corresponding metadata, what these disclosures have shed light on is the vulnerably of most information and the ease at which it may be gathered. The adage derived from the classic New Yorker cartoon with the caption, 'On the Internet, no one knows you're a dog', no longer holds. Your home, the color and shine of your fur, your breed and breakfast can now easily be ascertained. Yet, judging by the reactions in the media, it seems many individuals and institutions were ignorant of the fact that so much personal and sensitive information is out there for the taking. Indeed, as John Naughton writes in the Guardian:

'If anyone is shocked by what's been disclosed in the last fortnight, then they haven't been paying attention to the technology. Computer power has been obeying Moore's Law – doubling every two years – for nigh on four decades. Network bandwidth has been tripling every year. Ditto digital storage capacity. The result is that what looked like science fiction 20 years ago is now a mundane reality.'[4]

Similarly, German politician Malte Spitz last year quite clearly explained what can be done with metadata.[5] Spitz could, on the basis of his own data requested from his services provider, reconstruct his every move made over the course of 6 months. To show the German public what data retention policies mean and make possible, he produced a visualization of his life over this period.[6] The fact that knowledge of what could be done with such information was available to the public before the eavesdropping events of 2013 yet that, internationally, no major interest groups or political parties mobilized to raise awareness regarding internet policy and civil right justifies Naughton's argument that 'it's not just citizens who are behind the technological curve. Our political leaders seem similarly clueless'.[7]

This may seem to contradict what was written in the opening paragraph, but there is a distinct difference between the sensitive knowledge senior states(wo)men are privy to and the knowledge of parliamentarians or junior minister who will not possess any 'need to know'. Also there is difference between leaders receiving intelligence end products based on data trawling practices and senior politicians truly understanding the technical issues. For the German public at least, this was made obvious when German Chancellor Angela Merkel described the internet as 'new' and 'uncharted territory'.[8] Governments and parliamentarians exist to represent citizens, but if both the citizens and representatives do not understand the scope of technological change, there is a problem for society. When politicians do not possess enough expertise to be able to propose adequate checks on intelligence services and companies, nor understand the implications and possibilities technological advances could have, this poses a threat to societies. Also if citizens do not comprehend these issues, they will not know when to call for change. The Snowden affair has

highlighted this worrying lack of knowledge regarding the architecture of the internet.

Digital Highways

The digital as well as physical internet is international by nature. The world's electronic communications pass through many places and the infrastructure and companies that support its transit along the information superhighway are often not under the jurisdiction of a single country. This includes the fiber-optic cables, internet exchange points and the many servers that host the cloud (only a small part of the network traffic goes through satellites). That is why the internet is often considered a global commons. The internet is therefore not just an ethereal cyberspace but it has a physical architecture, which, as former US Senator Ted Stevens has described and Andrew Blum elaborates on, consists of 'a series of tubes'.[9]

The allegations by Snowden suggest that the UK is tapping over 200 internet cables that, due to the historic and geographic circumstances, converge on the British Isles.[10] Yet this capability is not just one that could be possessed by the UK, the US or France or other western countries. Given the proliferation of communication cables that have traversed the globe as these maps from Telegeography shows,[11] there are many places around the globe where these cables, that carry the internet and telecoms data, make landfall. One US diplomatic cable (note that this type of correspondence derives its name from the very channels by which it used to be transmitted: submarine cables) released by Wikileaks emphasizes their importance as crucial infrastructure to the US and definitely for many others.[12] It is therefore probable to assume that any country that harbors a cable landing site and possesses sufficient technical prowess can tap into the digital sea lines of communication. Der Spiegel estimates that

'[r]oughly half a dozen countries maintain intelligence agencies like the NSA that operate on a global scale. In addition to the Americans, this includes the Russians, Chinese, British, French and — to a lesser extent — Israelis and Germans. They have all placed the Internet at the heart of their surveillance operations.'[13]

This being said, cables do not necessarily need to make landfall on or traverse a nation's territory as a prerequisite for access. According to Snowden, the US gained access to a firm with headquarters in Hong Kong, which owns extensive submarine cable networks in the Asia-Pacific.[14] Moreover, tapping into the tubes does not only occur when cables make landfall. As former NATO Supreme Allied Commander Europe James Stavridis pointed out,

'the use of "underwater drones" might someday allow […] the exploitation of underwater fiber-optic cables deep on the ocean floor. This could one day provide a rich environment for intelligence collection, "blinding" communication pathways, and the conduct of cyber operations.'[15]

A similar practice was conducted during the Cold War by manned submarines.[16] The use of drones could make this process more prolific and less complex,[17] especially as in the future it is likely that there will be a proliferation of drone technology.

Exchange Points and Supply Chains

Cables are not the only crucial part of the cyber architecture; so too are internet exchange points (IXP), also known as the 'backbone' of the internet. These data choke points are located throughout the world, as this map by Telegeography shows.[18] Depending on their size, these exchanges handle local and regional traffic between internet service providers. They remove the need for data to take lengthy detours via overseas servers. The Chinese University of Hong Kong (CUHK) runs Hong Kong's key internet exchange (HKIX). Snowden alleges that the US gained access to this exchange, stating that '[w]e hack network backbones – like huge Internet routers, basically – that give us access to the communications of hundreds of thousands of computers without having to hack every single one'.[19] Similarly, Der Speigel describes how the Bundesnachrichtendienst (BDN), the German intelligence agency, monitors the largest hub in Europe located in Frankfurt.[20] Snowden's revelations furthermore led members of the Netherlands House of Representatives to ask one of the biggest IXP in Amsterdam to provide clarification on the practices, consequences and legal frameworks related to the possibility of wire-tapping of Internet

traffic.[21] Such practices may not even happen with the knowledge or consent of the companies operating cables, exchanges or other services. As one experts puts it,

'[t]he Internet is really driven by a series of transactions… [which] work because trust is the very foundation of the Internet. Having an unknown, unauthorized party access to what is essentially private communications erodes that trust, and with it, the very foundation of what makes the Internet work.'[22]

This is a trust that many companies would not think of jeopardizing, although some media outlets inferred that alleged access gained by the US to HKIX could indicate a backdoor into the systems though a built-in function in the hardware operated there.[23] Similar concerns about this type of cyber-attack via backdoors in software and hardware lay at the base of separate warnings made by the US House Intelligence Committee and the UK Intelligence and Security Committee, who expressed concern about awarding infrastructure contracts to certain Chinese telecoms giants.[24] This problem is, however, endemic to the defense, communications and technology industries given the globalized nature of supply chains.[25] Governments and corporations will need to continue to put more emphasis on the security of their global software and hardware supply chains. Large-scale electronic information-gathering of the type disclosed by Snowden need neither be unique nor limited to Western agencies. Again, it is plausible to presume that with sufficient knowhow and resources any country could partake in this data free-for-all.

Education

Ultimately, people will need to develop a greater understanding of the physical and digital geography of data. As storage capacity has increased, private companies, for their own purposes and often with our consent, have gathered increasing amounts of information on their clients. Timothy Garton Ash notes that '[t]his commercial accumulation of intimate personal information is worrying in itself.'[26] For one reason, we have seen in recent years that this very personal information has gotten into the hands of criminals who have hacked into companies such as Sony and Linkedin amongst others.[27] For another reason, Ladar Levison, the owner of the now defunct encrypted email service provider Lavabit warned that 'without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.'[28]

Most recently, many have realized just how much access governments and companies may have to personal information. What was predicted by Malte Spitz came to fruition with the revelations of PRISM and XKeyscore.[29] This type of information gathering gives organizations and governments the power to survey societies, to see what they are up to, what networks and groups are doing and which individuals are most active within them. This information is very sensitive and can be a powerful tool to be used for the good of society i.e. by protecting it from terrorist threats and espionage; but it can also be used as a more nefarious tool for totalitarian governments to control their societies and pick out those who are standing up for their rights.

It is perhaps lucky that many of the governments mentioned in connection with these eavesdropping affairs are democratic and accountable governments. This is because their citizens will have the opportunity to ask questions, push for reforms and gain more transparency about what access is given to private information and how their civil liberties will remain guaranteed. Awareness must be raised among those who will be affected by digital policy making, but who will have little knowledge of technical issues and the ways in which data can be collected and used. It is partly up to governments to provide transparency and a basic understanding of data retention and partly up to the citizens to learn about technology, its consequence for society and civil rights. Spitz, for example, calls for citizens to claim their digital self-determination. Functioning and accountable democratic governments should be constrained by a desire to protect civil liberties. Yet it is highly probable that less accountable but technologically-advanced regimes are conducting similar programs. What would have happened if such data trawling programs were at the disposal of authoritarian regimes during the Arab spring, the Velvet revolution or the Color revolution?

Even so, the internet is a global phenomenon. The servers that host it store personal data throughout the globe and can be accessed by other governments than the one the owner of the information is represented by. As a result,

citizens will need to be more aware of the risks that could come with imparting their information to the internet where access to their data is not only regulated by the laws of their own country, due to the fact that data travels over different line and across geographic lines to get to their destinations and as many companies are multinational. As Gen Hayden noted

'Let's keep in mind that in a global telecommunications infrastructure, geography doesn't mean what it used to mean…The Internet lacks geography, so I wouldn't draw any immediate conclusions with regard to some of those numbers that have been put out there as to who's being targeted and who isn't.'[30]

Indeed, what is most worrying is the lack of understanding among the general public of the implications of society's ever-increasing reliance on the digital world. The EU Justice Commissioner Viviane Reding called the surveillance a wake-up call for us to advance on our data protection reform for both the private and the public sector.[31] Indeed, it is important that the international community, politicians, businesses and citizen alike take stock of the current state of affairs and increase their awareness of cyber security. Programs should be started or reinforced to educate students, employees and citizens. The benefits of the digital age have come to us so easily and swiftly that many adults and adolescents have not been sufficiently educated in their secure use. Digital illiteracy is a growing problem.

Yes, our younger generations are growing up enjoying an array of digital devices, but many do not understanding what personal information not to share, nor do they have the ability to effectively and critically evaluate how to use information. As Ben Hammersley recently noted in the Guardian: 'The most important life skill we'll be teaching our children over the coming decades will be cyber-hygiene.'[32] The knowledge of how computer infections take place and what to do about them will be essential. Moreover, coding and other cyber skills are highly sought after in job markets, yet there is an increasing lack of cyber skills. The young and old seem inadequately prepared, and lack the necessary understanding of technology, cyber awareness, information security and skills to operate effectively in cyber space.[33] Finally, communications skills will become essential when trying to bridge the gap between young and old, initiated and uninitiated. Given the technical nature of the subject matter, communicating its impact clearly and intelligibly to (possibly less cyber-aware) senior-level staff, who are responsible for important decisions regard cyber affairs, will be crucial.

Conclusion

Given the degree of technological surprise felt by many, this seems more than necessary as those responsible for the regulation of information technology and infrastructure may, at present, not be able to adequately understand and address these issues. As Paul Kurtz, who served on the US National Security Council explains, '[m]ost people don't realize how information moves around the globe… and there are vulnerabilities all along the line'.[34] The fact remains that on different levels, data from governments, corporations and citizens will remain vulnerable due to the very geography of the net and the fact that, to many, it is simply terra incognita. As this article has argued, it is of vital importance that people and politicians alike now make the effort to critically explore this terrain in order to gain an appreciation for how data can be collected, how it can be used and ultimately, how it can be protected.

—

Henry Philippens *is currently an independent security and defense analyst. He has worked at numerous international organizations and think tanks and has published on international security issues. He holds MA degrees International Relations and History, respectively from the War Studies Department – King's College London and from the University of Leiden.*

[1] For example, at the Press Conference of the 46th Foreign Ministers' meeting, post ministerial conferences, 20th ASEAN Regional Forum and 3e East Summit Foreign Ministers' meeting, US Secretary of State John Kerry responded to allegations of US bugging of the EU stating that; 'I will say that very country in the world that is engaged in international affairs of national security undertakes lots of activities to protect its national security and all kinds of information contributes to that and all I know is that that is not unusually for lots of nations' (http://www.youtube.com/watch?v=_2RMYY8HLzY). The former Netherlands' Foreign Minister, Ben Bot commented

that espionage is of all times and that he was aware of being under surveillance by foreign powers ('Ben Bot: ik werd ook afgeluisterd', *Nederlandse Omroep Stichting*, July, 1 2013 http://nos.nl/l/tcm:5-1738142/

Philipp Wittrock,' NSA Spying in Germany: How Much Did the Chancellor Know?', *Der Spiegel*, July 03, 2013 http://www.spiegel.de/international/germany/how-much-did-merkel-know-about-nsa-spying-in-germany-a-909174.html). Former CIA and NSA Director Gen. Michael Hayden commented 'The United States does conduct espionage'… 'Any European who wants to go out and rend their garments with regard to international espionage should look first and find out what their own governments are doing' (Lindsey Boerma, 'Former NSA, CIA director: "The United States does conduct espionage"', *FacetheNation – cbsnews,* June 30, 2013 http://www.cbsnews.com/8301-3460_162-57591682/former-nsa-cia-director-the-united-states-does-conduct-espionage/) [2] Christopher Williams, 'Jacqui's secret plan to 'Master the Internet', *The Register*, May 3, 2009 http://www.theregister.co.uk/2009/05/03/gchq_mti/ Last accessed: August 7, 2013; Christopher Williams, 'GCHQ: Mastering the Media – Spy agency in public equivocation shocker', *The Register*, May 5, 2009 http://www.theregister.co.uk/2009/05/05/gchq_mti_statement/ Last accessed: August 7, 2013; 'Government 'not planning to monitor all web use', *The Telegraph*, May 4, 2009 http://www.telegraph.co.uk/technology/news/5271796/Government-not-planning-to-monitor-all-web-use.html Last accessed: August 7, 2013; Ko Colijn, 'Ophef over afluisteren terecht?', Nieuwsuur uitzending, July, 1 2013 http://nos.nl/l/tcm:5-1738330/; Duncan Campbell, *"They've got it taped – Somebody's listening"* New Statesman, August 12, 1988. [3] At a news conference in Tanzania US President Barak Obama explained; 'I think we should stipulate that every intelligence service — not just ours, but every European intelligence service, every Asian intelligence service, wherever there's an intelligence service — here's one thing that they're going to be doing: they're going to be trying to understand the world better and what's going on in world capitals around the world from sources that aren't available through the New York Times or NBC News; that they are seeking additional insight beyond what's available through open sources', Office of the Press Secretary – The White House, Remarks by President Obama and President Kikwete of Tanzania at Joint Press Conference at State House Dar es Salaam, Tanzania, July 01, 2013 http://www.whitehouse.gov/the-press-office/2013/07/01/remarks-president-obama-and-president-kikwete-tanzania-joint-press-confe [4] John Naughton, 'If you think GCHQ spying revelations don't matter, it's time to think again', *The Guardian*. June 22, 2013, http://www.guardian.co.uk/commentisfree/2013/jun/22/gchq-internet-snooping-Kafkaesque [5] Malte Spitz, 'Your phone company is watching' Speech held at *TEDGlobal* 2012, July 24, 2012 http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching.html; Malte Spitz, 'Tell-all telephone' *ZEIT-Online*, 2012 http://www.zeit.de/datenschutz/malte-spitz-data-retention [6] Malte Spitz, 'Tell-all telephone' *ZEIT-Online*, 2012 http://www.zeit.de/datenschutz/malte-spitz-data-retention [7] John Naughton, 'If you think GCHQ spying revelations don't matter, it's time to think again', *The Guardian.* June 22, 2013 http://www.guardian.co.uk/commentisfree/2013/jun/22/gchq-internet-snooping-Kafkaesque [8] Park MacDougald, 'Angela Merkel Discovers the Internet — and Inspires a Meme', *Foreign Policy*, June 20, 2013 [9] Andrew Blum, *Tubes: A Journey to the Center of the Internet* (New York 2012); 'It's a series of tubes', is the infamous explanation of the internet given by former US Senator Ted Stevens'Series of tubes', Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc., date last updated (May 30, 2013), sate accessed (July, 04 2013) http://en.wikipedia.org/wiki/Series_of_tubes [10] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian*, June 21, 2013, http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [11] Telegeography, *Submarine Cable Map* Last Accessed: July 4, 2013 http://www.submarinecablemap.com/; Telegeography, *Global Internet Map*, 2009 http://www.telegeography.com/assets/website/images/maps/global-internet-map-2009/global-internet-map-2009-x.jpg [12] 'Critical Infrastructure and Key Resources Located Abroad Request For Information: Critical Foreign Dependencies', WikiLeaks. WikiLeaks cable: 09STATE15113, February 18, 2009 http://wikileaks.org/cable/2009/02/09STATE15113.html [13] 'The German Prism: Berlin Wants to Spy Too', *Der Spiegel*, June 17, 2013 http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html [14] Lana Lam and Stephen Chen, 'Snowden reveals more US cyberspying details', *South China Morning Post*, June 23, 2013 http://www.scmp.com/news/hong-kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed; Lana Lam, 'US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009', *South China Morning Post*, June 23, 2013 http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator [15] James Stavridis, 'The New Triad – It's time to found a U.S. Cyber Force', *Foreign Policy*, June 20, 2013 .http://www.foreignpolicy.com/articles/2013/06/20/the_new_triad [16] 'Operation Ivy Bells', Wikipedia: The Free

Encyclopedia. Wikimedia Foundation, Inc., date last updated (May 30, 2013), site accessed (July, 04 2013) https://en.wikipedia.org/wiki/Operation_Ivy_Bells [17] 'Exploring the oceans 20,000 colleagues under the sea', *The Economist*, 07 June 2012 http://www.economist.com/node/21556551 [18] Telegeography, *Internet Exchange Map* Last Accessed: July 4, 2013 http://www.internetexchangemap.com/ [19] James Pomfret, 'Ex-CIA man's snooping claims raise alarm bells in Hong Kong', *Ruiters* June 13, 2013 http://www.reuters.com/article/2013/06/13/us-usa-security-hongkong-idUSBRE95C08920130613 [20] 'The German Prism: Berlin Wants to Spy Too', *Der Spiegel*, June 17, 2013 http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html [21] 'Official reaction of AMS-IX to statements in the media and questions by Dutch Parliament regarding wire-tapping of Internet traffic' *Amsix – Amsterdam Internet Exchange*, June 11, 2013 https://www.ams-ix.net/newsitems/91; 'Gespreksnotitie AMS-IX ten behoeve van het rondetafelgesprek d.d. 26/6/13 van de vaste commissie voor Binnenlandse Zaken van de Tweede Kamer over de praktijken, gevolgen en wettelijke kaders inzake het aftappen van persoonsgegevens', *Amsix – Amsterdam Internet Exchange*, June 26, 2013 https://www.ams-ix.net/newsitems/95 [22] Byron Holland, 'NSA, Prism and Internet Exchange Points in Canada', *CircleID,* 21 June 2013 http://www.circleid.com/posts/20130621_nsa_prism_and_internet_exchange_points_in_canada/ [23] Teresa Leung, 'CUHK: No detection of hacking into HKIX', *Computer World Hong Kong*, June 13, 2013 http://cw.com.hk/news/cuhk-no-detection-hacking-hkix [24] 'UK ministers defend Chinese deals after security risk warning', *BBC News*, June 6, 2013 http://www.bbc.co.uk/news/uk-politics-22795226'Huawei and ZTE deny US spying charges at hearing', *BBC News*, September 14, 2012 http://www.bbc.co.uk/news/business-19595778 [25]John Reed, 'The U.S. Might Be Buying Weapons With Enemy Access Built In', *Foreign Policy*, July 22, 2013 http ://killerapps.foreignpolicy.com/posts/2013/07/22/the_us_might_be_buying_weapons_with_enemy_access_built_in?wp_login_redirect=0 [26] Timothy Garton Ash, 'If Big Brother came back, he'd be a public-private partnership',*The Guardian*, June 27, 2013 http://www.guardian.co.uk/commentisfree/2013/jun/27/big-brother-public-private-partnership-nsa [27] '2012 LinkedIn hack', Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc., date last updated (June 12, 2013), date accessed (August, 11 2013) http://en.wikipedia.org/wiki/2012_LinkedIn_hack; 'PlayStation Network outage', Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc., date last updated (July 17, 2013), date accessed (August, 11 2013) http://en.wikipedia.org/wiki/PlayStation_Network_outage [28] Ladar Levison, 'Letter written on the occasion of the closure of Lavabit', August 9, 2013 http://lavabit.comLast accessed: August 12, 2013 [29] Glenn Greenwald, 'XKeyscore: NSA tool collects 'nearly everything a user does on the internet'', *The Guardian*, July 31, 2013 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [30] Lindsey Boerma, 'Former NSA, CIA director: "The United States does conduct espionage"', *FacetheNation – cbsnews,* June 30, 2013 http://www.cbsnews.com/8301-3460_162-57591682/former-nsa-cia-director-the-united-states-does-conduct-espionage/ [31]'Joint EU-US group to assess US spy ops', *BBC News*, July 3, 2013 http://www.bbc.co.uk/news/world-europe-23165257 [32] Wang, Norcie, Komanduri, Acquisti, Leon & Cranor, '"I regretted the minute I pressed share":A Qualitative Study of Regrets on Facebook', *Symposium on Usable Privacy and Security (SOUPS),* July 20–22, 2011, Pittsburgh, PA USA http://www.guardian.co.uk/technology/2013/jun/16/future-of-behaviour-concepts-for-21st-century?CMP=twt_gu [33] Karen Evans & Franklin Reeder, 'A Human Capital Crisis in Cybersecurity – Technical Proficiency Matters',*A Report of the CSIS Commission on Cyber Security for the 44th Presidency*, November 2010 http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf Robert Hinck, 'For Hire: Cybersecurity Specialist', *The Center for Strategic and International Studies (CSIS)* http://csis.org/blog/hire-cybersecurity-specialist [34] James Geary, 'Who Protects The Internet?', *Popular Science,* March 13, 2009 http://www.popsci.com/scitech/article/2009-03/who-protects-intrnet?single-page-view=true

---

About the author:

Henry Philippens is currently an independent security and defense analyst. He has worked at numerous international organizations and think tanks and has published on international security issues. He holds MA degrees International Relations and History, respectively from the War Studies Department – King's College London and from the University of Leiden.