Should network usage be monitored by government to support national defence?

JACK FURBY
CM2302
November 15, 2017

1 Introduction

In September 2007 the US's National Security Agency (NSA) started a program called PRISM which monitors communications between the US and foreign nationals over the internet (Arthur 2013). This program includes a number of large technology companies including Google and Apple and requires them to turn over data when required. This was the full content of the data and not just meta data. This is all done without the user, who the data associates to, ever knowing about it. As much as this should not result in anyone being surveyed unreasonably this program was only discovered in 2013 and potentially, has taken data from both US citizens and citizens of other nationalities as data from other countries would often "flow through the U.S" (*PRISM slides* 2013). In this essay I will defend the argument that network usage should not be monitored by governments to support national defence.

2 How network usage is monitored

When using a computer network your traffic will be routed on the cheapest path. This is almost certainly means that whilst in the UK is going to end up on the UK's fibre backbone that connects the UK with the rest of the world. Here GCHQ via the TEMPORA program were found in May 2013 to be collecting vast amounts of data (up to 21 petabytes a day) by tapping fibre-optic cables (MacAskill et al. 2013). GCHQ in 2013 had over 200 cables tapped and was able to listen to "46 of them at a time" (MacAskill et al. 2013). All of this data would then be stored for review. As the taps were at major network locations all network usage would be captured. As expected most of this data captured would be normal network usage and only a small sliver would actually contain valuable information for national defence. In addition GCHQ would be getting your data without any permission to do so. It would only be after review when they would decide if they were right to get the data. This as it stands should not be the case. For someone to gain access to your house, such as a police officers, they either need to be invited in or have a warrant signed by a court. The same could be said for networks since they contain the same, if not more personal, data about someone. As it stands with TEMPORA it's as if the police officer has gone into your house, had a look around and then left (as long as they did not find anything) without you even knowing they'd been there.

Another method the government uses to monitor network usage is via companies themselves. These are companies by the likes of Google, Apple, Dropbox etc who work a lot from the data they collect. One way they are doing this recently came to light when again, the UK government has been found analysing "Millions of Facebook and Twitter accounts" (Briggs 2017). The exact data collected in this case is unclear but GCHQ accessed the companies containing the data databases. This kind of data gathering process has been used before such as when PRISM forced companies to hand over data requested. In GCHQ's case however it seems to be on a far wider scale with entire databases accessed. Whether the companies were forced in this case is unclear but even if they were it is also likely they cannot comment on their involvement. Accessing this data is incredibly invasive on the public's privacy as this may include data such as location, private messages, pictures etc as almost every social media companies collects this data. With this the government will know almost everything there is about you and your location while this may allow them to know where criminals are, it is nerveless an incredible invasion of privacy. As much as this is now within the scope of the law its hard to see how knowing where everyone works and lives helps narrow down on the criminals (who the true target should be).

The final method by which the governments collects network usage is by the use of Black boxes which have been installed and used since 2016 to collect meta data (White 2012). The meta data collected is stored for one year for all internet traffic. The method by which this takes place is that all data for a single request is looked at, the content is discarded and the meta data is saved. This is even possible on some encrypted data such as emails. This is alarming as it also leads to the potential for all data to be saved since the system could be modified to keep the content of the data. It is a legal requirement for ISP's to use black boxes. The data collected using this method can be accessed on demand by services such as the police, without a warrant. What this does is allow the system to be abused, for example by employees of an organisation with access to the data to use it for their own gain. This would be a breach of the data protection act. On top of this it is easy to bypass this system with the use of a VPN resulting in a lot of the targets this system is after finding a way round it only leaving regular citizens left to be monitored.

3 What data is collected and what happens to it

PRISM, TEMPORA, social media access and black boxes all give us a good understanding of what data is collected to support national defence. The range is vast with TEMPORA collecting just about everything, along with PRISM, as they both tap cables carrying data. Social media access potentially gives the government access to our private messages, location history, views on politics and likes and dislikes and finally the black boxes provide the government with meta data about our data e.g. websites visited and when they were visited. Going back to relating the collection of data to search warrants. All of this data is collected without ones knowledge. For Police to obtain a warrant to search a property they have to "convincing a neutral and detached magistrate" (Nolo n.d.) which means the police must provide written evidence showing they have a probable cause to a judge or magistrate who will look over the evidence and, if they consider the evidence enough a search warrant will be granted. With network monitoring none of this need be put into place. The government will simply just come up with solutions to get what they need and not let the owner of the data or anyone else aware of what they are doing. This has even gone as far as the overseeing body of GCHQ, in the case of getting data from social media, by cutting department head out of the loop (Briggs 2017). As things stand these acts should be against the law and warrants necessary to access this content or information from network communications.

With all this data a lot happens with it. First off a lot of it is shared. This includes a number of government run services including the police and NHS but also includes Bristol University (Briggs 2017) which is given the entire database of social media data. This is an incredibly worrying fact as this is putting personal data in the hands of not only services to support national defence but research and health institutes. As to what this data is then used for and if it anonymised is unclear but, no matter what individuals from whom this data originated from did not give consent to their data being taken, let alone used, by a 3rd party. Another area this data ends up is in the hands of overseas organizations such as the NSA (MacAskill et al. 2013). As much as GCHQ and the NSA may be following the law for data sharing outside of the EU what if there are other organizations GCHQ has shared data with who does not follow these rules. The main principle of the Data Protection Act is "Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data" (unknown 1998) in relation to sharing data outside of the EU. Considering how long some of the network surveillance projects go on without the public knowing it is highly possible data has been shared against the law that these organisations should be enforcing. If we are trusting government to defend us they should be leading by example and not hiding their practices from the people they are trying to protect especially when they involve them.

4 Data storage

Network usage creates a lot of data. This then has to be stored either in full, like TEMPORA does with storing all data for 3 days, or meta data which is what your ISP will be doing. As this data is all personal this poses a big risk if someone manages to hack the database storing the data. In my research I could not find a government database containing the public's personal data that had been hacked but to understand what sort of scale this might be we can look at the Equifax hack. There has been two hacks to Equifax in the past year. In total these have resulted in 143 million US citizens data and 400,000 UK citizens data being taken. This included names, address, phone numbers, national security numbers and even driving licence details (Hern 2017). If this hack happened to a government controlled database containing data collected from monitoring network usage we could see something on the same scale of this or larger. The result could potentially be a large risk in identity theft which itself may involve peoples bank accounts being emptied and loans taken in their name. Traditionally with this kind of breach everyone affected would be notified by law but with a number of governments programs to collect data being top secret (at least to start with) if one of these had a data breach it seems unlikely the breach would also be top secret and the affected would never know. It is in fact possible that this has already happened but we just don't know it yet. This goes in completely the opposite direction to helping national defence. With data like that taken in the Equifax hack there was a chance enough information would be taken about an individual for a passport to be created by a terrorist or similar which would then allow them to travel to the US or other western country.

The chance of a major hack happening to a government database you would hope is unlikely but no matter the system it is always possible to break in (especially if the systems have to be connected to a network in order to function). This is because computer systems run by organisations often are running old software. This include the Navy in the UK who still runs windows XP (Boyle 2017). Microsoft stopped supporting this product in 2014 leaving the Navy and any other systems running Windows XP open to exploits that may yet be undiscovered. In addition of old software, zero days (vulnerability in a piece of software that the vendor does not know about) can be used to exploit a device. These will have no known fix when found which hackers can use to break into a system. With the data network surveillance stores for national defence the first someone would know about this kind of exploit is unauthorised access and, depending on the severity of the exploit there may be little that can be done to stop data and other services being affected. As mentioned above, the data stored is highly sensitive and keeping it secure must be a high priority. With all the programs mentioned so far which monitor network usage they all have one trait in common which is they all share data. The exact figures are unknown but considering any organisation should have at lease 3 copies in case one is corrupt or lost and with all ISP's in the UK having storage, the number of machines to access data quickly adds up. This all adds more points of entry for malicious activity. All it takes is for one of these servers not to be updated or patched and a potential threat is created.

5 Does it work?

With all these programs being targeted (or at least from what we are told) terrorism and other crimes need to be stopped before it is a threat. The result of all of this, as reviewed by Congress, an open court and two independent White House panels have all come back as negative with respect to threats stopped in the case of US programs such as PRISM (Helen 2014). This proves there is no need for the invasion of privacy as it results in no strengthening to national defence and will just cost the tax payer more money that could be put to far better use.

Another example of why surveillance is harmful for national defence can be see in an article by Fortune who includes a section about the opinion of Coleen Rowley a former FBI special agent. It states "if locating terrorist plotters is akin to finding a needle in a haystack, Rowley insists, the last thing we should do is keep adding more hay" (Solomon 2015). What this is saying is it is hard enough to keep track of criminals with just targeting the ones we know and suspect. What the government is doing is trying to solve the problem with more data with almost all of it being irrelevant. As a result we need more analysts to sift through the data at the expense of our privacy. Again this will cost the public with more taxes and no gain to national defence.

My final point is even with monitoring network traffic, if the data being transmitted is captured and if it is encrypted (possible with messaging apps such as iMessage on iPhone) and passed over a virtual private network (VPN) or transmitted over the TOR network there is very little surveillance can do about it. Any criminal with minimal knowledge about staying private will know about these technologies and therefore use them. All of the technologies can be used for free or with a small cost and especially in the case of VPN's are widely advertised (a simple Google search showed that nordVPN is a secure VPN which can be used to hide your data usage). The result of this is the surveillance will just capture everyone of no interest to the government and leave most of the real criminals alone.

The technologies mentioned above will use encryption of some form or another. Messaging services will often use end-to-end encryption so you know what application sent the information but not what the information is. A VPN will put your data through an encrypted tunnel so only the initial handshake will be unencrypted and everything else including what site you visit will be encrypted. TOR on the other hand will encrypt your data and pass it through the TOR network so anyone spying on the traffic will not be able to work out where the packets originated.

6 Conclusion

In conclusion I believe the government should not monitor our network usage as it is an invasion of privacy and evidence shows it does not work. I don't think the government will ever stop surveillance but the implementation should have is an open approach where their programs are known by the public and unless somebody is suspected of criminal activity somebodies personal network usage and data associated with it is not monitored or stored at all. If you are suspected of committing criminal activities a warrant will be required for surveillance to start. This would mean everyone with nothing to hide will not be unnecessary watched.

References

Arthur, C. (2013), 'Nsa scandal: what data is being monitored and how does it work?', *The Guardian* . Available at: https://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions [Accessed: 2017-10-15].

Boyle, D. (2017), 'Hms queen elizabeth is 'running outdated windows xp', raising cyber attack fears'. Available at: http://www.telegraph.co.uk/news/2017/06/27/hms-queen-elizabeth-running-outdated-windows-xp-software-raising/ [Accessed: 2017-10-25].

Briggs, B. (2017), 'Uk spy agencies share social media data with foreign governments, say critics', *The Ferret* . Available at: https://theferret.scot/uk-spy-agencies-share-social-media-data-foreign-governments-say-critics/ [Accessed: 2017-10-19].

Helen, W. (2014), 'We don't have to give up liberty to have security: Edward snowden at ted2014'. Available at: https://blog.ted.com/we-dont-have-to-give-up-liberty-to-have-security-edward-snowden-at-ted2014/ [Accessed: 2017-10-25].

Hern, A. (2017), 'Equifax: credit firm was breached before massive may hack'. Available at: https://www.theguardian.com/technology/2017/sep/19/equifax-credit-firm-march-breach-massive-may-hack-customers [Accessed: 2017-10-25].

MacAskill, E., Borger, J., Hopkins, N., Davies, N. & Ball, J. (2013), 'Gchq taps fibre-optic cables for secret access to world's communications', *The Guardian* . Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed: 2017-10-19].

Nolo (n.d.), ‘Search warrants: What they are and when they’re necessary’, *Nolo* . Available at: https://www.nolo.com/legal-encyclopedia/search-warrant-basics-29742.html [Accessed: 2017-10-20].

PRISM slides (2013). Available at: https://nsa.gov1.info/dni/prism.html [Accessed: 2017-10-15].

Solomon, N. (2015), ‘Why government surveillance won’t protect your data’. Available at: http://fortune.com/2015/08/26/cybersecurity-nsa-att/ [Accessed: 2017-10-25].

unknown (1998), ‘Data protection act 1998’. Available at: https://www.legislation.gov.uk/ukpga/1998/29/schedule/1 [Accessed: 2017-10-20].

White, G. (2012), “black boxes’ to monitor all internet and phone data’, *Channel 4* . Available at: https://www.channel4.com/news/black-boxes-to-monitor-all-internet-and-phone-data [Accessed: 2017-10-20].