HBCS CW4

Cybersecurity Ethics

Student ID: 2136685

Table of Contents

Table of Figures

1. Ethical Challenges

In recent times, a large quantity of products made are connected to the internet, expanding the ever-growing sea of Internet of Things (IoT). These products all require cybersecurity, therefore proportionally expanding the field of cybersecurity as the IoT sea is expanding as well. This makes the cybersecurity field a vast horizon of different practices and different ethical challenges for each practice. For example, the practice of cloud security, network security, or physical security; they all come with different ethical challenges.

Common ethical challenges arise for organisations, such as the ethics of conducting penetration tests to increase network security and/or physical security, or privacy-invasive procedures for the sake of cybersecurity - however sometimes this reason is used as a scapegoat for mass surveillance. Other issues exist such as resource allocation, for example, in hospitals. Great cybersecurity comes at a cost, and slicing a big part of the budget on it, while neglecting sectors such as personal protective equipment can be morally wrong. Moreover, having a time-consuming login procedure before accessing life-saving equipment in a critical situation where every second matters, can be the determining factor between a patient living or dying (Swiss Cyber Institute, 2021).

A large and overarching ethical problem is mass surveillance by governments. Thanks to the global surveillance disclosures from approximately 2013, we now know how involved the U.S. is with secret surveillance projects. The Director of National Intelligence in the United States said that these projects were crucial to national security and that the disclosures jeopardised it (Gardner and Hosenball, 2013).

On the other hand, projects of mass surveillance have been the sole reason criminals such as child predators have been identified. For example, the crack down of a child pornography Tor onion service and the more than 1000 computers that accessed the website by the FBI (Condliffe, 2016; Floyd, 2017; Paganini, 2016).

The U.S. encroach on ordinary people’s private lives and gather sensitive information unbeknownst to anyone, using backdoors and vulnerabilities that the NSA describes as “NOBUS” – “nobody but us” (Computer Hope, 2020; Peterson, 2013). For example, it is approximated that the mass surveillance of the NSA has covered approximately 75% of the internet traffic in the U.S. at the time of the global surveillance disclosures in 2013 (Newell, 2014).

Below are a few bullet-pointed examples of mass surveillence projects exposed:

- The FBI distributed viruses and keyloggers that anti-virus softwares such as Network Associates Inc. (parent company of McAfee at the time) and Symantec (parent company of Norton and AVAST) choose not to detect, such as the Magic Lantern keylogger (Kaspersky, 2001).

- Major American tech companies such as Google and Microsoft provided the NSA with internet communications and security vulnerability information, allowing them to conduct Zero-Day attacks before revealing them to the public with the help of the Tailored Access Operations (TAO) Team and the PRISM project. The details collected can be seen in Figure 1 and the participating companies can be seen in Figure 2 (Schneier, 2013).
- The NSA's TAO team intercepted shippings of devices purchased online and installed "beacons" in them, before delivering them to the target's address, as seen in Figure 3 (Gallagher, 2014; Spiegel, 2013).
- The CIA's Mobile Devices Branch found exploits in smartphones running iOS and Android – and weaponised Android vulnerabilities - with the help of GCHQ and NSA (WikiLeaks, 2017a; WikiLeaks, 2017b; WikiLeaks, 2017c).
- The CIA and MI5 developed a tool called "Weeping Angel". Discovered by WikiLeaks, Weeping Angel was used to hack into early Samsung smart TVs and enable their in-built microphones and video cameras, if available, all while the TV appeared to be off (WikiLeaks, 2017c; WikiLeaks, 2017d).

2. Public Obligations of Cybersecurity Professionals

Cybersecurity professionals are there to ensure the security of a company's information, allowing the company to conduct business as usual, and on the other hand, ensuring that sensitive information isn't accessible by threat actors.

Whenever a data breach does occur, leaking customers' private information, a professional should inform the public as soon as possible so that they can do damage control, such as freezing bank accounts and changing passwords, as this is the ethical solution. However, some cybersecurity professionals choose to keep the breach a secret to keep the company's reputation intact and to avoid paying fines such as the GDPR fine of up to 20 million euros, or 4% of annual worldwide turnover, whichever is higher (Intersoft Consulting, 2018).

Some cybersecurity professionals would like to disclose the breach to the public but the company may not let them to, resulting in a conflict of interest and a personal ethical dilemma for the professional. The professional may want to disclose it anonymously, but they may not be able to risk their workplace due to economical reasons. The ones that do choose to disclose the unethical practices, called whistleblowers, may face social, economical and political backlash, such as Julian Assange and Edward Snowden. The former facing extradition to the U.S. and up to 175 years in prison and the latter leaving for Russia, the U.S.' adversary, after publishing top-secret NSA documents in 2013 (Republic World, 2022; Reuters, 2022).

Cybersecurity professionals have access to people's sensitive data and they are entrusted with it. If a professional had no ethics and morals, they could steal it and sell it whenever they would like. However as a professional with an obligation to the public, they must have a strong sense of ethics and respect for people's privacy (Reciprocity, 2021).

As there are always new technologies and new vulnerabilities being developed, cybersecurity professionals must always have their systems updated to the newest version to ensure that vulnerabilities have been patched. A professional that does not update their systems while knowing that they are putting sensitive information at risk is unethical and it cannot be justified as software updates are usually free-of-charge. Even if the the systems must be upgraded by puchasing new hardware or software, it is the professional's public obligation to keep the information safe.

On the other hand, if a cybersecurity professional is developing a security tool, it is very unethical to purposely implement backdoors in the software and then publish it to the public as a trustworthy program. For example, see the U.S. projects discussed in the previous chapter.

3. Equifax Case Study

The Equifax 2017 data breach exposed the personal details of approximately 150 million people, including names, addresses, social security numbers and even credit card numbers. The breach occurred due to a vulnerability in a software used by Equifax called Apache Struts, discovered in early March of 2017. The developers of the Apache Struts developed a fix on the 7th of March and on the 9th of March, Equifax system administrators were notified to patch their vulnerable software, however they dismissed the warning as their vulnerability scanners told them that none of their machines were vulnerable (epic.org, 2021; Fruhlinger, 2020; Ullrich, 2017).

The same month of March, Equifax was notified of suspicious activity, by a partner company called Mediant who also had the same vulnerability, of threat actors using stolen social security numbers from Mediant to log into Equifax. Mediant warned Equifax of the vulnerability as well, however they didn't report any significant activity until May of 2017 (Fruhlinger, 2020).

From May to July of 2017, threat actors were able to gain access to multiple databases and steal the millions of records of sensitive information. The treat actors encrypted their traffic when stealing the data to make it more difficult for Equifax to realise what was stolen. However, Equifax could decrypt their network traffic, however they required a valid certificate, which they haven't renewed for nearly 10 months (Fruhlinger, 2020).

Not only did Equifax fail to minimise the damage appropriately, their public response was met with criticism, and deservedly so. Equifax announced their breach in September of 2017, 7 months after the vulnerability was discovered and 5 months after they started seeing unauthorised activity, unethically keeping their customers in the dark about the security of their information. The announcement came alongside a website called “equifaxsecurity2017.com”, holding information for those affected. However, this domain looked very familiar to those used for phishing scams so the customers would be very skeptical in typing in personal information. Moreover, the Equifax social media redirected people to “securityequifax2017.com”, which wasn’t bought at the time, and luckily was bought by a person redirecting people to the real website. The domain could’ve easily been bought by a threat actor attempting to phish information from already upset customers. The real website allowed customers affected to check if their information was affected, however when checking, customers waive their rights to sue Equifax for the data breach, unethically making people choose between getting justice and getting compensation for the damages (epic.org, 2021; Fruhlinger, 2020).

The Equifax cybersecurity team could have been following the company policy, or orders from the CISOs, however the fact that the software patch was free of charge, the dismissal in March of 2017 and the late applying of the patch can only be seen as negligent and goes against the public obligations of a cybersecurity professional. The failure of the executive team can be confirmed by the fact that a large majority of the C-suite executives resigned quickly after the breach was announced. On the other hand, the late reveal to the public of the breach was deeply unethical and has caused Equifax to lose trust. Moreover, after customers checking if they were affected, Equifax offered credit protection for a price, only showing how Equifax prioritises financials over the people’s data that allows their business to run, showing how unethical they are. (epic.org, 2021; Fruhlinger, 2020; Kerbs on Security, 2017; Ng, 2018).

4. References

Computer Hope (2020). *What is NOBUS?* [online] www.computerhope.com. Available at: https://www.computerhope.com/jargon/n/nobus.htm [Accessed 22 Apr. 2023].

Condliffe, J. (2016). *FBI Refuses to Divulge How It Tracked Pedophiles on Tor*. [online] Gizmodo. Available at: https://gizmodo.com/fbi-refuses-to-divulge-how-it-tracked-paedophiles-on-to-1767933079 [Accessed 22 Apr. 2023].

epic.org (2021). *EPIC - Equifax Data Breach*. [online] archive.epic.org. Available at: https://archive.epic.org/privacy/data-breach/equifax/ [Accessed 23 Apr. 2023].

Floyd, J. (2017). *FBI's 'Network Investigative Technique' in Child Porn Cases*. [online] www.johntfloyd.com. Available at: https://www.johntfloyd.com/fbis-network-investigative-technique-child-porn-cases/ [Accessed 22 Apr. 2023].

Fruhlinger, J. (2020). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* [online] CSO Online. Available at: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html [Accessed 23 Apr. 2023].

Gallagher, S. (2014). *Photos of an NSA 'upgrade' factory show Cisco router getting implant*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/ [Accessed 22 Apr. 2023].

Gardner, T. and Hosenball, M. (2013). Spy agency seeks criminal probe into leaks. *Reuters*. [online] 9 Jun. Available at: https://www.reuters.com/article/us-usa-security-clapper-idUSBRE9570GL20130609 [Accessed 22 Apr. 2023].

Greenwald, G. and MacAskill, E. (2013). *NSA Prism program taps in to user data of Apple, Google and others*. [online] The Guardian. Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [Accessed 22 Apr. 2023].

Intersoft Consulting (2018). *General Data Protection Regulation (GDPR) – Final text neatly arranged*. [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/issues/fines-penalties/ [Accessed 22 Apr. 2023].

Johnson, K., Martin, S., O'Donnell , J. and Winter, M. (2013). *NSA taps data from 9 major Net firms*. [online] USA TODAY. Available at: https://eu.usatoday.com/story/news/2013/06/06/nsa-surveillance-internet-companies/2398345/ [Accessed 22 Apr. 2023].

Kaspersky (2001). *The FBI's 'Magic Lantern' Shines Bright*. [online] www.kaspersky.com. Available at: https://www.kaspersky.com/about/press-releases/2001_the-fbi-s--magic-lantern-shines-bright [Accessed 22 Apr. 2023].

Kerbs on Security (2017). *Equifax Breach Response Turns Dumpster Fire*. [online] kerbsonsecurity.com. Available at: https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/ [Accessed 23 Apr. 2023].

Newell, B.C. (2014). *THE MASSIVE METADATA MACHINE: LIBERTY, POWER, AND SECRET MASS SURVEILLANCE IN THE U.S. AND EUROPE*. [online] Available at: https://cdn.netzpolitik.org/wp-upload/SSRN-id2339338.pdf [Accessed 22 Apr. 2023].

Ng, A. (2018). *How the Equifax hack happened, and what still needs to be done*. [online] CNET. Available at: https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/ [Accessed 23 Apr. 2023].

Paganini, P. (2016). *FBI must reveal the network investigative technique used to hack more than 1000 computers*. [online] Security Affairs. Available at: https://securityaffairs.co/44687/cyber-crime/fbi-network-investigative-technique.html [Accessed 22 Apr. 2023].

Peterson, A. (2013). Why everyone is left less secure when the NSA doesn't help fix security flaws. *Washington Post*. [online] 4 Oct. Available at: https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/ [Accessed 22 Apr. 2023].

Reciprocity (2021). *The Importance of Ethics in Information Security*. [online] Reciprocity. Available at: https://reciprocity.com/the-importance-of-ethics-in-information-security/ [Accessed 23 Apr. 2023].

Republic World (2022). *Why is WikiLeaks founder Julian Assange facing 175 years in prison? What are US' charges?* [online] Republic World. Available at: https://www.republicworld.com/world-news/uk-news/why-is-wikileaks-founder-julian-assange-facing-175-years-in-prison-what-are-us-charges-articleshow.html [Accessed 22 Apr. 2023].

Reuters (2022). Putin grants Russian citizenship to U.S. whistleblower Snowden. *Reuters*. [online] 27 Sep. Available at: https://www.reuters.com/world/europe/putin-grants-russian-citizenship-us-whistleblower-edward-snowden-2022-09-26/ [Accessed 22 Apr. 2023].

Schneier, B. (2013). *How the NSA Thinks About Secrecy and Risk*. [online] The Atlantic. Available at: https://www.theatlantic.com/technology/archive/2013/10/how-the-nsa-thinks-about-secrecy-and-risk/280258/ [Accessed 22 Apr. 2023].

Spiegel (2013). *The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks - DER SPIEGEL - International*. [online] www.spiegel.de. Available at: https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html [Accessed 22 Apr. 2023].

Swiss Cyber Institute (2021). *A Holistic Approach to Ethical Issues in Cyber Security*. [online] Swiss Cyber Institute. Available at: https://swisscyberinstitute.com/blog/a-holistic-approach-to-ethical-issues-in-cyber-security/ [Accessed 22 Apr. 2023].

The Guardian (2013). *NSA Prism program slides*. [online] The Guardian. Available at: https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document [Accessed 22 Apr. 2023].

Ullrich, J. (2017). *Critical Apache Struts 2 Vulnerability (Patch Now!)*. [online] SANS Internet Storm Center. Available at: https://isc.sans.edu/diary/22169 [Accessed 23 Apr. 2023].

WikiLeaks (2017a). *Android Exploits and Techniques*. [online] wikileaks.org. Available at: https://wikileaks.org/ciav7p1/cms/page_11629096.html [Accessed 22 Apr. 2023].

WikiLeaks (2017b). *iOS Exploits*. [online] wikileaks.org. Available at: https://wikileaks.org/ciav7p1/cms/page_13205587.html [Accessed 22 Apr. 2023].

WikiLeaks (2017c). *Vault 7*. [online] Wikileaks.org. Available at: https://wikileaks.org/ciav7p1/ [Accessed 22 Apr. 2023].

WikiLeaks (2017d). *Weeping Angel (Extending) Engineering Notes*. [online] wikileaks.org. Available at: https://wikileaks.org/ciav7p1/cms/page_12353643.html [Accessed 22 Apr. 2023].

5. Appendix

5a. Equifax Case Study

In the summer of 2017, it was revealed that Equifax, a massive credit reporting bureau managing the credit rating and personally identifying information of most credit-using Americans, had suffered a severe security breach affecting 143 million Americans.[1] Among the data stolen in the breach were social security and credit card numbers, birthdates, addresses, and information related to credit disputes. The scale and severity of the breach was nearly unprecedented, and to make things worse, Equifax's conduct before and after the announcement of the breach came under severe criticism.

For example, the website created by a PR consulting firm to handle consumer inquiries about the breach was itself riddled with security flaws, despite requesting customers submit personally identifying information to check to see if they were affected. The site also told consumers that by using the site to see if they were affected, they were waiving legal rights to sue Equifax for damages related to the breach. The site, which gave many users inconsistent and unclear information about their status in the breach, offered to sell consumers further credit protection services from Equifax, for a fee.[2]

Soon it was learned that the Equifax had known of the May 2017 breach for several months before disclosing it. Additionally, the vulnerability the attackers exploited had been discovered by Equifax's software supplier earlier that year; that company provided a patch to all of its customers in March 2017. Thus, Equifax had been notified of the vulnerability, and given the opportunity to patch its systems, two months before the breach exposed 100 million Americans to identity theft and grievous financial harm.

Later, security researchers investigating the general quality of Equifax's cybersecurity efforts discovered that on at least one of Equifax's systems in Argentina, an unsecured network was allowing logons with the eminently guessable 'admin/admin' combination of username and password and giving intruders ready access to sensitive data including 14,000 unencrypted employee usernames, passwords and national ID numbers.[3]

Following the massive breach, two high-ranking Equifax executives charged with information security immediately retired, and the Federal Trade Commission launched an investigation of Equifax for the breach. After learning that three other Equifax executives had sold almost two billion dollars of their company stock before the public announcement of the breach, the Department of Justice opened an investigation into the possibility of insider trading related to the executives' prior knowledge of the breach.[4]

1 https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/

2 https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

3 https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/

4 https://www.engadget.com/2017/09/18/equifax-stock-sales-doj-investigation-insider-trading/

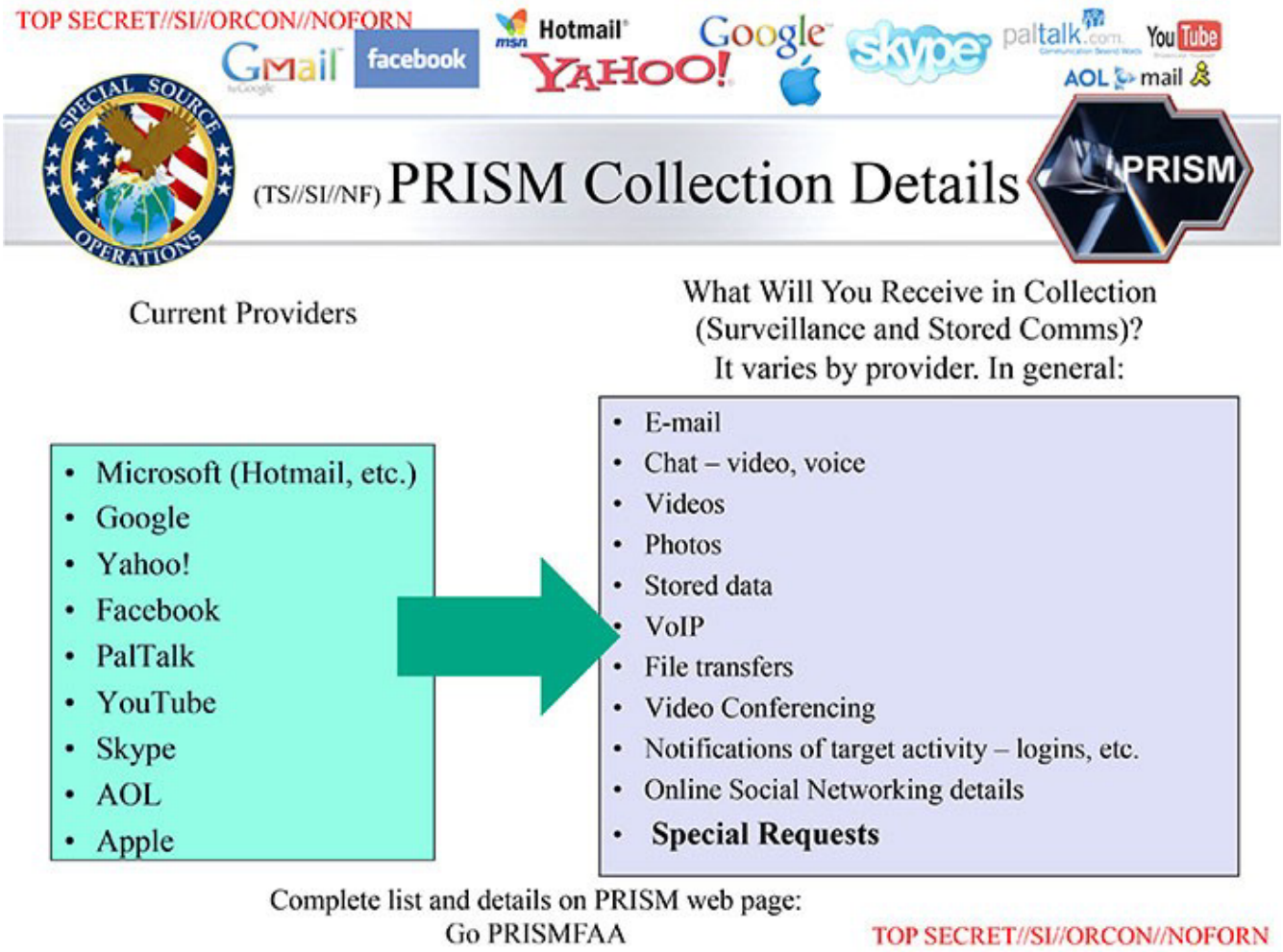

Figure 1: PRISM Collection Details (The Guardian, 2013)

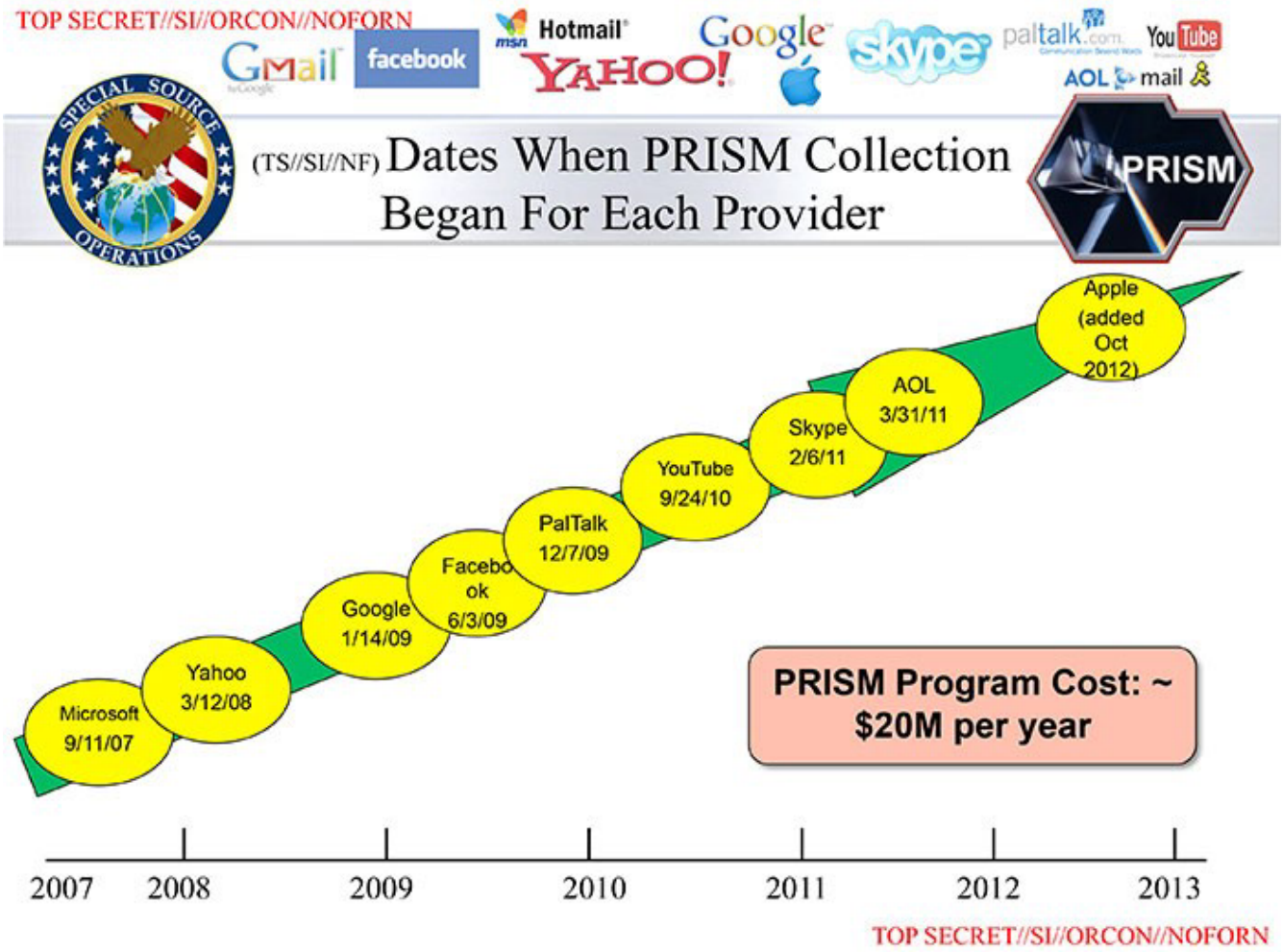

Figure 2: PRISM Beginning Collection Dates (The Guardian, 2013)

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Figure 3: TAO Team opening a parcel to install a "beacon" (Gallagher, 2014)