Legal, social and ethical issues in Vault 7, WikiLeaks claims

Abstract

Vault 7 has like other leaks from WikiLeaks aroused a chain of ethical, social and legal issues not only with the US and other governments all over the world but also within the major companies that manufacture and maintain major hardware and software like Apple, Google, Microsoft, Samsung and Linux as well as private citizens. Specifically, it raised the issue of private data safety in mainstream gadgets such as personal computers, Smart TVs and Smartphone. Legal issues largely touch on the freedoms and civil rights of individuals and citizens and their relationship with the civil, private and criminal law. Ethical issues are tied to legal and social issues and will center on the rightfulness or wrongfulness of invasion of privacy by the government through justifications of security. Finally, social issues revolve around the impacts being felt by masses due to their privacy being invaded. The conclusion of the discussion shows that in as much as freedom and civil liberties are constitutionally protected; they should not limit the government's primary duty of protecting its citizens and protecting its borders. For this reason, citizens have to adapt to the use of surveillance technology and the legal system should be fine tuned to accommodate the practice. However, the government should ensure that the practice is ethical.

Table of Contents

Abstract 2

Introduction 4

Part 1: Reactions from affected parties 4

Part 2: Legal, social, and ethical issues relating to the leak by WikiLeaks and the CIA's hacking operations? 5

Legal issues 5

Ethical issues 8

Conclusion 11

Reference List 12

Appendices 15

Introduction

Vault 7 has like other leaks from WikiLeaks aroused a chain of ethical, social and legal issues not only with the US and other governments all over the world but also within the major companies that manufacture and maintain major hardware and software like Apple, Google, Microsoft, Samsung and Linux as well as private citizens. The leaks contained nearly 9,000 files which contained sensitive information from the CIA. Besides it is alleged the CIA had secretly developed ways to conduct surveillance on private citizens through their electronic devised such as Smart TVs and Smartphone. The issue of surveillance has increasingly raised concerns over its legality especially with the widely recognised rights to privacy as enshrined in most democratic nation's constitution as well as in international law.

Similarly, the debate around the lawfulness of the practice has continued to trigger debate regarding its social impact. Citizens have started to doubt their governments and its practices in infringing on their fundamental rights. Finally, combining the legal and social issues arising from the issues, more concerns have emerged about the ethical and moral foundations of the practice. This it is important to critically evaluate these three elements using Vault 7 as a reference point.

Part 1: Reactions from affected parties

The Vault 7 Wikileaks affected key players in the hardware and software industry including Apple, Google, Microsoft, Samsung, and Linux. Specifically, it raised the issue of private data safety in mainstream gadgets such as personal computers, Smart TVs and Smartphone. In their reaction, these major players reassured the public on the safety measures that have been undertaken to safeguard personal data that is stored in their personal gadgets and electronics using smart technology (Hern, 2017). For instance:

- **Apple** underlined that it had already remodeled the iOS vulnerabilities that were mentioned in the leaks which were similar to the communication delivered by Google which claimed that it had already fixed 'most' of the vulnerabilities. It is clear that the two firms did not deny the claims which strongly indicate that the technology most citizens are currently using is prone to the threats identified in the leaks.
- According to Khandelwal (2017) hardware, giant and manufacturer of home appliances such as TV **Samsung** equally reacted through a defensive message stating that its top priority was on protecting the privacy and security of consumers of its brand. Acknowledging its awareness of the leaks by WikiLeaks the firm maintained that it was investigating the matter.
- **Linux**, the owners of a widely used operating system, globally stated that even if it was targeted just like other players its open source feature enables it to fix vulnerabilities and release the fixes promptly to users (Gunnar, 2017).
- Conversely, the accused **(US government through the CIA)** maintained that the primary role of the agency was to collect intelligence which is used to protect the US from foreign threats such as terrorism. A report by the BBC explained that the CIA, however, refuted the claim that it was conducting domestic surveillance of American citizens stating that the leaks intended to furnish its credibility and ability to protect Americans from foreign attacks (The BBC, 2017).

Part 2: Legal, social, and ethical issues relating to the leak by WikiLeaks and the CIA's hacking operations?

Legal issues

The massive unearthing and publishing of private and confidential information such as the CIA's "Vault 7" by WikiLeaks are likely to attract legal implications touching on the publisher and the government agency. The first legal aspect that emerges strongly in such a

situation is how the privacy of information of individuals and agencies is easily breached. Notably, the "Vault 7" WikiLeaks case provides a complex situation where CIA (an intelligence body) purports to gather information covertly for purposes of its homeland security but perceived to infringe the privacy of people. Ideally, the U.S. Constitution (fourth amendment) protects individuals from intrusion by government and private agencies in case their privacy is compromised (Legal Information Institute, n. d.). Interestingly, intelligence and security agencies such as CIA would want least to have even a byte of their information revealed to the public.

On the other hand, they try their best to source information from all over the world in innovative and complex ways that individuals cannot realise. Most individuals are not aware of these practices by agencies like CIA hence they are disadvantaged even when their rights are not respected. Essentially, WikiLeaks seems to be playing the role of informing ignorant people about the breach of their private life but at a "legal cost." One important legal provision that comes to the fore in the said leaks is the Electronic Communications Privacy Act signed into law in 1986 (Public Broadcasting Service, 2014). According to this act, "the ECPA protects against the unlawful interceptions of any wire communications--whether it's a telephone or cell phone conversations, voicemail, email, and other data sent over the wires" (Public Broadcasting Service, 2014, para 9). Often, consumers use electronic devices that are infested by programmes and codes from intelligence agencies like CIA but they are not aware. More so, their private communication details can be tapped and relayed to CIA without their consent as indicated in the "Vault 7" leaks. This contravenes the ECPA and privacy rights stipulated in the constitution.

At the same time, WikiLeaks takes a great risk in publishing sensitive information sourced from privy sources sometimes working in these agencies. It goes back to breach of private and confidential information in addition to malicious intentions and homeland

security threat. A security intelligence body like the CIA would argue that publishing such sensitive information is likely to compromise homeland and global security. A decision by WikiLeaks and such other parties to publish such information without the consent of CIA implies conspiracy (Feruza and Kim, 2007).

The UN, as well as international law, recognises the right to privacy. More so, key privacy principle in today's laws is established through Article 12 of Universal Declaration of Human Rights (UDHR). The article declares no person should be subjected to an unwarranted invasion of their privacy, their homes or families or associates neither shall their reputation or honor is subjected to arbitrary invasion. Besides, the clause maintains that every person has a right to be protected against such attacks or invasions through existing laws. On the same, the 1990 *UN Guidelines for the Regulation of Computerized Personal Data Files* outlines the *Fair Information Practices* which advised nations to implement regulations concerning personal privacy protection. Additionally, privacy protection is considered a basic human right, essential to safeguarding liberty.

As noted by William Pfaff, totalitarianism is best defined through its characteristic of assaulting privacy. From the current case, it is evident that the US government through the CIA has continued to ignore the basic requirements of the law (Risen and Savage, 2010). Although the CIA denies conducting surveillance practices on American citizens, it is evident from the leaks that it is true. Thus, the government through its agencies is depriving citizens' privacy consequently destroying their liberty.

In the UK the *Investigatory Powers Bill* which was recently passed by parliament has left citizens in the country vulnerable to surveillance practices by the government. If assented, the bill will legalise the global surveillance initiatives/ programs by the UK government. The surveillance involves data from private communications anywhere in the world

communications (Cohen, 2003). More so, it will allow the state to have access to information on UK citizens and to store such information subsequently. Specifically, the law will empower spies from the UK to hack citizens and their internet infrastructure where the government considered necessary. The law further requires telecommunication and internet companies to store the records of communications and policies will not be required to seek a warrant to access the information. However, in the past, even case law considered evidence collected without a warrant inadmissible in a court of law. The *Regulation of Investigatory Powers Act 2000* (RIPA) maintains that evidence collected through intervention is inadmissible during trial. Further, the Act fails to criminalise the benefits associated with the use of the collected evidence. This is justified by the fact that most works of investigation as done in secret and therefore making the benefits of secretly collected evidence would handicap the investigating bodies.

Therefore, the main legal issue in the current case involves the impact of evidence collected through surveillance. First, will it be admissible in court if applied under the current laws? If it cannot be used against the criminals of what significance is it given the high costs associated with the practice? Then solutions to these questions have been positively supported by the *Investigatory Powers Bill* given that it empowers investigative bodies to collect, use and store private data gathered through surveillance.

Ethical issues

The identified legal implications of the Vault 7 leaks by WikiLeaks gives rise to additional issues that are ethical. Whereas, the law may be based on facts and is widely applied to maintain law and order, ethics is concerned more about what is right or wrong. Thus, the key ethical issue, in this case, concerns determining whether it is right to intrude the privacy of citizens (foreign or domestic) (Wu et al., 2015). On the other hand, it is right to ignore sufficient leads that help reduce or stop a criminal act that would otherwise injure or cause

death the many innocent citizens? The primary role of intelligence agencies like the CIA is to collect evidence though secretes methods with the intention of using such intelligence to protect citizens. Their responsibilities are justified since they protect and reduce criminal acts all over the world. Nonetheless, the ethical dilemma emerges not only from the lawfulness of hacking phone calls and internet communications/data but on whether the private and public liberties are safe or being exploited by obsessive governments, through justifications of national security.

Another concern against the government's practice of hacking personal computers and appliances the use smart technology is that it allows it to push the boundaries of the process gain uncontrolled power. This deliberate abuse of power by the government is unethical and unacceptable, especially in democratic spaces. Critics of surveillance through privacy invasion argue that in fact, governments already have too much power that needs to be kept in check and not augmented. Consequently, it is only in the constitution that the government is prevented from abusing such powers. Referring to the blatant misuse of these powers by the government in the past, they maintain that a reconsideration of the laws to allow the government the authority to surveillance foreign citizens will open loopholes to even their citizens.

Therefore, the ethical consideration in the current case remains a dilemma to both sides in the argument. On one side, citizens need protection from foreign and domestic attacks, and hence they believe that it is the responsibility to apply whatever means possible to realize this obligation. On the other hand, it is argued that citizens have a right to privacy and hence it is not only illegal to allow the government to interfere but also unethical. Accordingly, the truth can only be established somewhere in between. The government should not be limited regarding the extent to which it should protect its citizens. Nonetheless, such powers must be balanced delicately so that they do not invade the privacy of citizens they are safeguarding.

Social issues

Citizens have continued to show a division regarding their views on the trade-off between the right to privacy and their security needs. The Vault 7 leaks have reignited the debate on the extent to which the government should be allowed to invest in surveillance through hack technology/applications. In a research conducted by Pew, it was shown that most citizens favoured the "security first" consideration and were willing to sacrifice their liberty for security (Rainie et al., 2016). This trend is nearly universal where citizens support at least some extra measures by the intelligence and law enforcement communities due to the increased terror attacks even though it may adversely invade their privacy. Lerner (2015) observes that the continued disclosure of invasive surveillance by Wikileaks, the Snowden revelations and now the recent vault 7 leaks have resulted in the development of a chilling effect on citizens.

Accordingly, this has forced individuals to modify or change their behaviour to conform to modern social and political order simply because they acknowledge that they are being observed (Gilliom and Monahan, 2013; Rainie and Madden, 2015). Regardless of the technique used, most people now prefer to meet face to face, and in places, they are sure to have no or minimal surveillances such as rooftops or better yet to use handwritten documents whose trails can be permanently erased. Although the majority agree that they are open for surveillance considering they have nothing to hide, it can no longer be assumed that they are skeptical of using their smartphones or other personal gadgets without the thought of being observed crossing their mind.

The moment individuals are aware that their private lives are intruded, they will tend to be more secretive and suspicious. They are considering that the CIA has turned to use sophisticated software on electronic devices such as TVs, mobile phones, and computers to the source for private information means that individuals have to be more cautious. In

response, people are likely to shift their preference to brands from other countries, for instance, the Chines and South East Asia products with an assumption that their probability of infestation is low. Correspondence through platforms such as emails, texting, and online chatting is likely to reduce especially countries that are suspect to be a source of global security threat. Citizens of such countries are likely to cope with skewed information because of strict government controls in fear of espionage. Sometimes, they are locked from what is happening around the world because major mass media and information channels are cut off. Individuals no longer trust security agencies that are meant to protect their rights to privacy and confidentiality; rather, they become more suspicious of such bodies in light of massive leaks like "Vault 7". Internationally, countries no longer trust each other as was the case of the tapping of the German Chancellor by the U.S. intelligence services (The Guardian, 2015).

Conclusion

According to the collected evidence, invasive surveillance cannot be ignored in modern society. It has been justified by the presence of increased insecurity especially major crimes such as terrorism. Besides, it is noted that white collar crimes are also on the rise and the only effective way to curb its effect is through increased online surveillance. The Vault 7 documents that revealed how the CIA has been conducting invasive surveillance not only abroad, but even within the US, has generated mixed reactions from the affected parties. For instance, the software and hardware manufacture reacted by reassuring citizens that they have addressed the vulnerabilities identified in previous versions of their technologies. On its part, the government underlined that it had a primary duty to protect its citizens at whatever cost. Thus, the case in itself presents three key issues-legal, ethical and social. Accordingly, with nations like the UK enacting laws that allow the government to conduct surveillance both domestically and abroad, it will be no surprise if other nations follow suit, the US included.

Reference

Article 12 of Universal Declaration of Human Rights (UDHR)

Cohen, T. (2003). ISPA Advisory 10: The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002.

Gilliom, J. and Monahan, T. (2013). *SuperVision*. 1st ed. Chicago: The University of Chicago Press.

Feruza, S. and Kim, T. (2007). IT security review: privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, 2(2), pp. 17-32. Available at: http://www.sersc.org/journals/IJMUE/vol2_no2_2007/2.pdf

Gunnar, U. (2017). *Wikileaks Vault 7 Highlights Importance of Tech Self-Sufficiency*. [online] Global Research. Available at: http://www.globalresearch.ca/wikileaks-vault-7-highlights-importance-of-tech-self-sufficiency/5579039 [Accessed 10 Apr. 2017].

Hern, A. (2017). *Apple to 'rapidly address' any security holes as companies respond to CIA leak*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2017/mar/08/wikileaks-cia-leak-apple-vault-7-documents [Accessed 10 Apr. 2017].

Khandelwal, S. (2017). *7 Things That Happened After WikiLeaks Dumped The CIA Hacking Files*. [online] The Hacker News. Available at: http://thehackernews.com/2017/03/cia-wikileaks-hacking.html [Accessed 10 Apr. 2017].

Legal Information Institute (n. d.). Fourth Amendment. Cornell University Law School, n. p. Available at: https://www.law.cornell.edu/constitution/fourth_amendment

Lerner, M. (2017). *The Chilling Effect of Domestic Spying*. [online] Americanpolicy.org. Available at: https://americanpolicy.org/2014/08/05/the-chilling-effect-of-domestic-spying/ [Accessed 11 Apr. 2017].

Lyon, D. (2013). *The Electronic Eye*. 1st ed. New York, NY: John Wiley & Sons.

Public Broadcasting Service (2014). Computer crime laws. *PBS*, n. p. Available at: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

Rainie, L. and Madden, M. (2015). *Americans' Views on Government Surveillance Programs*. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2015/03/16/americans-views-on-government-surveillance-programs/ [Accessed 11 Apr. 2017].

Rainie, L., Maniam, S., Rainie, L. and Maniam, S. (2016). *Americans feel the tensions between privacy and security concerns*. [online] Pew Research Center. Available at: http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ [Accessed 11 Apr. 2017].

Rainie, L., Maniam, S., Rainie, L. and Maniam, S. (2016). *Americans feel the tensions between privacy and security concerns*. [online] Pew Research Center. Available at: http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ [Accessed 11 Apr. 2017].

Risen, C. and Savage, C. (2010). *Federal Judge Finds N.S.A. Wiretaps Were Illegal*. [online] Nytimes.com. Available at: http://www.nytimes.com/2010/04/01/us/01nsa.html [Accessed 11 Apr. 2017].

Rotenberg, M. (2014). *Preserving Privacy in the Information Society*. [online] Unesco.org. Available at: http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm [Accessed 10 Apr. 2017].

The BBC, (2017). *Apple, Samsung and Microsoft react to Wikileaks' CIA dump - BBC News*. [online] BBC News. Available at: http://www.bbc.com/news/technology-39203724 [Accessed 10 Apr. 2017].

The guardian (2014). NSA tapped German Chancellery for decades, WikiLeaks claims. www.theguardian.com, n.p. Available at: https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel

The Regulation of Interception of Communications and Provision of Communication related Act (RICA) of 2003

Tavani, H. T. (2007). Ethics & Technology: Ethical Issues in an Age of Information and Communication Technology (2nd Ed.). Hoboken, NJ: John Wiley and Sons, Inc

The Investigatory Powers Act 2016, UK

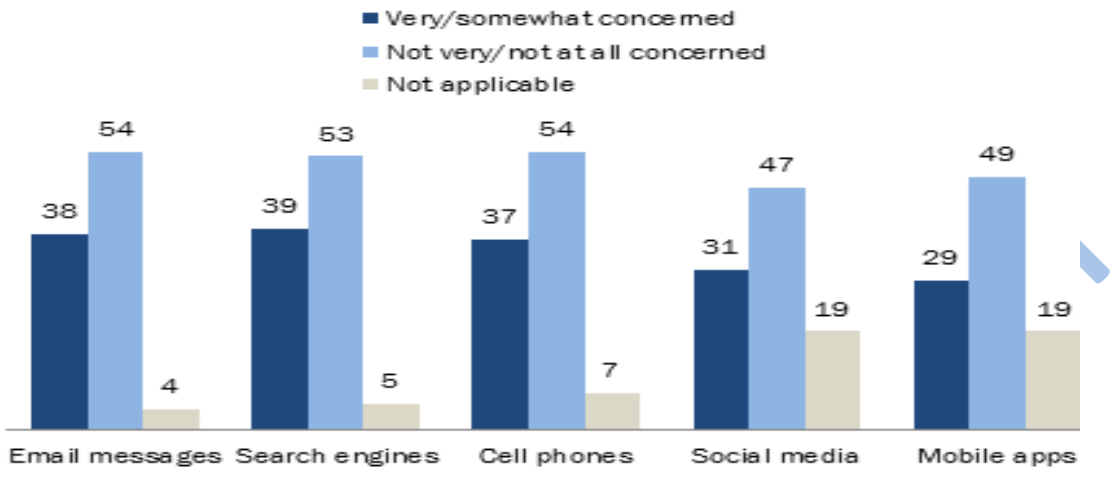
UN Guidelines for the Regulation of Computerized Personal Data Files of 1990

Wu, T., Chung, J., Yamat, J. and Richman, J. (2015). *The Ethics (or not) of Massive Government Surveillance*. [online] Cs.stanford.edu. Available at: https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html [Accessed 11 Apr. 2017].

Appendices

Americans Have More Muted Concerns about Government Monitoring of their Own Digital Behavior

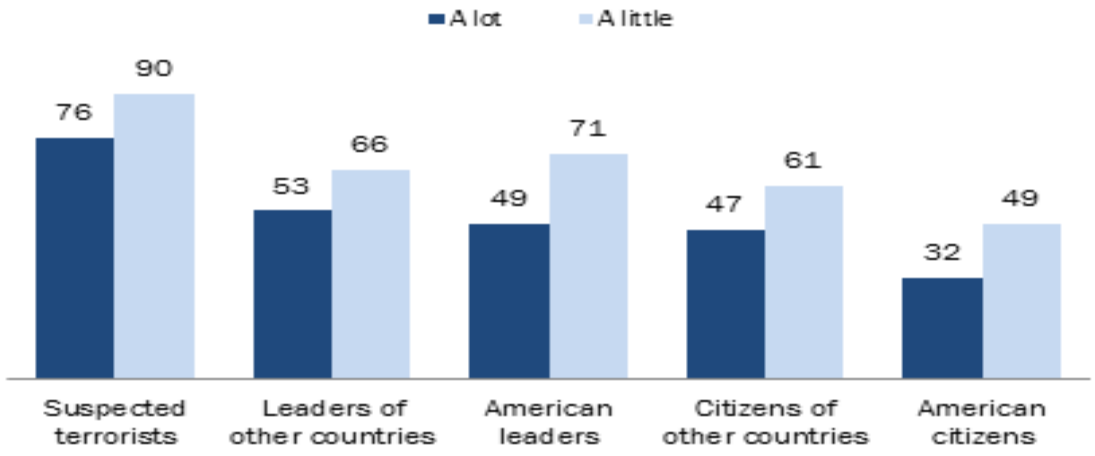
% of U.S. adults who say they are "very/somewhat" or "not very/not at all concerned" about government surveillance of their own data and electronic communications



Source: Survey of 475 U.S. adults on GfK panel November 26, 2014-January 3, 2015.,
PEW RESEARCH CENTER

Those Who Have Heard a Lot about Surveillance Programs Are Less Likely to Support Monitoring Others

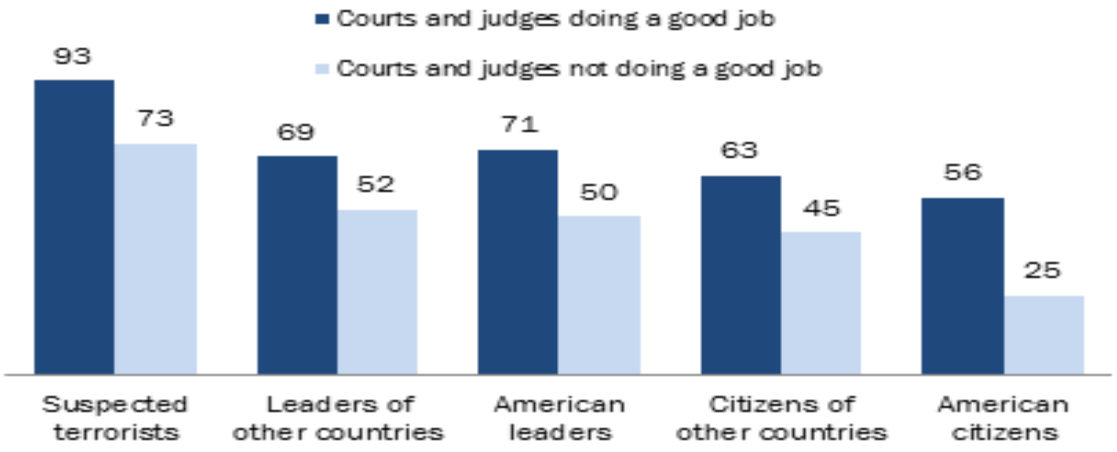
Among those who have heard "a lot" or "a little" about gov't surveillance programs, the % who say it is acceptable to monitor the communications of ...



Source: Survey of 475 U.S. adults on GfK panel November 26-2014-January 3, 2015.
PEW RESEARCH CENTER

Those Who Think the Judicial System is Doing a Good Job Balancing People's Privacy Rights with Law Enforcement Needs Are More Likely to Support Monitoring Others

Among those who think the courts and judges are doing a good job/not a good job, the % who say it is acceptable for the American gov't to monitor the communications of ...

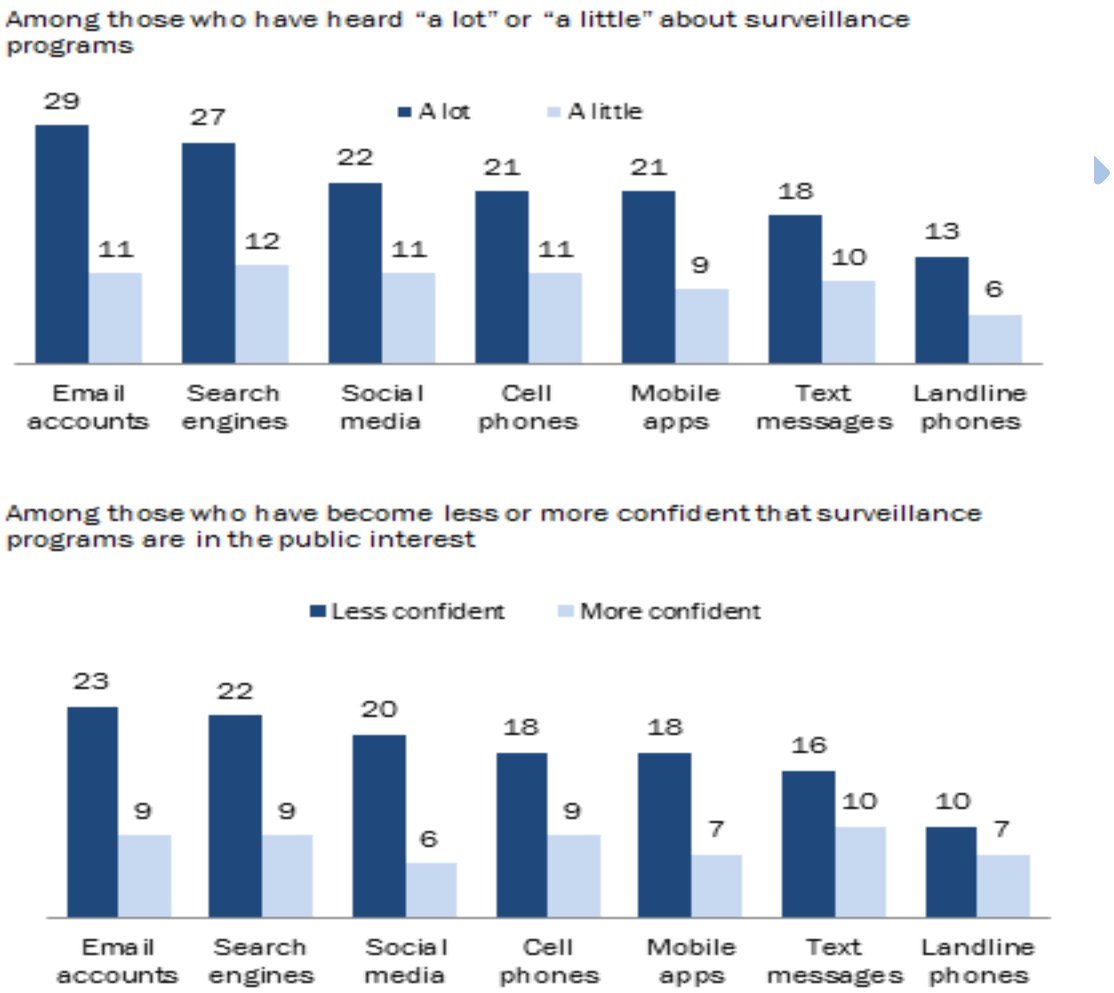


Source: Survey of 475 U.S. adults on GfK panel November 26-2014-January 3, 2015.

PEW RESEARCH CENTER

Those Most Likely to Have Changed Their Behavior on Technology Have Heard a Lot about the Surveillance Programs and Are Less Confident the Programs Are in the Public Interest

Among each subgroup, the % who say they changed their use of these technologies "a great deal" or "somewhat" since they learned of the phone and internet monitoring programs



Source: Survey of 475 U.S. adults on GfK panel November 26-2014- January 3, 2015.

PEW RESEARCH CENTER