Mass Surveillance and Internet Censorship Under Scrutiny

Ahmed Elsobky
0xsobky@gmail.com

Abstract

Since the very beginning of our digital age, it has been widely believed that national security and the right to privacy cannot possibly meet at a joining point; that way, we may only have one at the expense of the other. Internet censorship has also been utilised under the argument of blocking all sorts of unwanted digital materials. But when put under spotlight, such vague arguments and misconceptions all eventually start to dissipate into thin air.

Keywords: *Mass Surveillance, Internet Censorship, Privacy, IoT, Encryption.*

1. Introduction

We are living in a post-Snowden world where mass surveillance is being employed by various government agencies to monitor citizens indiscriminately under the argument of it being a necessity for national security. Definable as "the intricate surveillance of an entire or a substantial fraction of a population in order to monitor that group of citizens"—the practice of mass surveillance is such a global concern that raises a lot of unanswered questions.

Nonetheless, the issue of mass surveillance and its implications on our privacy is neither new nor it is particularly limited to a certain country or region. In the United States, for instance, the recent Snowden revelations reportedly exposed the existence of a wide variety of ongoing mass surveillance programs such as "PRISM," "X-Keyscore," and the list goes on. While in Australia, it was reported that 75 percent more government wiretap warrants have been issued than that in the United States during the year 2003 [1]. And in the United Kingdom, they have a notable spying program dubbed "Tempora" that was launched in 2011 amongst other programs too. Also in China, the Chinese government initiated the Golden Shield Project back in November 2003 in order to monitor and censor the Internet in the entire country. Yet in Russia, a system known as "SORM" was established as early as 1996 to monitor telephone communications which later has been extended to cover the Internet as a whole. And in India, the government there have had a wide range of surveillance systems capable of tracking online communications on a real-time basis by harvesting data from various voice-over-IP services, including Skype and Google Talk….

Not only that, but Internet censorship is also being utilised in both Western and Eastern countries to filter and block access to huge amounts of information on various web domains allegedly for blocking unwanted digital materials such as pornography and hate speech. Most recently, the unveiling of the Iranian "National Information Network," also known as "Halal Internet," that serves as a gateway to the World Wide Web. Reports indicate, too, that in the second half of 2014, Twitter alone has received a sum of 796 content removal requests—comprising about 80 percent increase than that in the previous year—and this number is only rising up drastically year after another [2].

2. Surveillance and Censorship in the Modern Age

Many recent leaks have made it very clear that multiple government agencies around the world are actively intercepting and analysing as much communications data as they possibly

can; it being Internet traffic or phone records, all sorts of telecommunications are being monitored around the clock.

Continuous developments in technology are driving us fast towards digitalisation where everything around us is connected. As much as new smart devices are introduced to make our lives easier—as per the Internet of Things hype—it opens a potential for a too transparent world where we are never free from surveillance. That way, data can be used to track and monitor people's behaviours almost everywhere, almost all the time.

And when it comes to Internet censorship, while a comprehensive regulation of online information would seem to be a very difficult task that requires non-trivial infrastructure from a technical point of view, new technologies that facilitate monitoring and filtering the flow of data online continue to emerge and advance over time.

3. Public Views on Mass Surveillance and Internet Censorship

According to a 2014 political typology survey by the Pew Research Center, a majority of American respondents disapprove the U.S. government's surveillance of Internet and telephone records—roughly 54 percent of them. While 74 percent of respondents said that they should not give up privacy and freedom for the sake of safety [3].

On another hand, in a 2012 survey conducted by Internet Society, about 30 percent of respondents believe that censorship does exist on the Internet. And around 66 percent of them agree that governments in countries with no Internet censorship whatsoever should have a responsibility to keep the Internet free of censorship in countries where the Internet is being censored. Additionally, more than 70 percent of respondents agree that the increase of government's involvement would make the Internet too controlled or would result in limiting content they can access. Nearly two-thirds of them also believe that increased government control would stifle innovation or rather undermine the growth of the Internet. And 83 percent of them agree that "access to the Internet should be considered a basic human right" [4].

However, based on surveys conducted in the MENA region in countries such as Egypt, UAE, Saudi Arabia, et al.—a majority of respondents agree that the Internet should be more tightly regulated with the exception of Tunisia where only 39 percent of respondents do support the former [5].

4. The Disjunction of Mass Surveillance and National Security

In a world where everybody is being watched, the allegation goes that people's privacy is significantly restricted in exchange for national security. But throughout the years, it proves very hard to find any tangible evidence that backs up or supports such claims of mass surveillance actually playing a big role in aiding counterterrorism efforts or preventing any major terrorist attacks in a given state or country. And from what we have seen, recent terror attacks have further exposed the inherent limitations of mass surveillance programs in effect.

On the contrary, some evidence was found to challenge the effectiveness of mass surveillance in contrast to traditional investigative methods. According to a report by the New America Foundation, the bulk collection of American telephone metadata seems to have played some role in initiating, at most, only 1.8 percent of all cases examined. While NSA's surveillance targeted at individuals outside of the United States—under Section 702 of the FISA Amendments Act—played a role in only 4.4 percent of all reviewed cases [6].

Nevertheless, we find government officials often exaggerating the role of mass surveillance in defending against terrorism, repeatedly calling for extending their monitoring systems capabilities and proposing restrictions on the use of encryption under the assumption of making the world a safer place as in the case of the recently passed Russian pair of bills—known as “Yarovaya Law”—which proposed new amendments to the pre-existing counter-terrorism laws there by further expanding the authority of law enforcement agencies and introducing new requirements for data collection and even cryptographic backdoors in the telecommunications industry [7].

5. Defects of Internet Censorship and Mass Surveillance

It’s a given that mass surveillance and Internet censorship both typically require vast amounts of resources to be dedicated in order for them to be conducted on any large scale. Notwithstanding, the effectiveness and efficiency of such programs are found to be in themselves very questionable.

Another major concern around Internet censorship is that it can be easily abused by repressive regimes to suppress freedom of expression—crippling the growth and diversity of the Internet. One instance of which was the silent blocking of WikiLeaks in both Turkey and Australia [8][9]. And in practical terms, censorship is found to be susceptible to either over-blocking or under-blocking issues, since that it is technically impossible to block just exactly targeted content at all times—meaning that access to permissible content on the Internet could get accidentally blocked by mistake and vice versa. One incident that demonstrates this point was the blocking of DailyMotion by Tunisian authorities in the year 2007 due to miscategorising it as pornography by the SmartFilter filtering software [10]. Another example would be when automatic censorship systems are set to block sexual content based on certain keywords such as “cunt”, mistakenly blocking content that contains neutral words like “scunthorpe” [11]. Or in cases when blocking an IP address of a shared hosting web server—that which hosts multiple websites—prevents access to all of them at once.

On the other side, it has been observed that the lack of transparency in developing and deploying mass surveillance tools could easily lead authoritarian regimes to abusively exploit their intelligence-gathering capabilities against dissident political activists and journalists. One example of which would be the “COINTELPRO" program that was conducted in 1956 by the United States Federal Bureau of Investigation (FBI) to spy on domestic political organisations [12]. Additionally, many concerns could be raised regarding potential false positive threats—and false negative ones too—that may arise during analysing the massive amounts of data collected.

Finally, the act of enforcing restrictions on and demanding for cryptographic backdoors in encryption systems would necessarily entail making us more vulnerable to cyber attacks conducted by non-state hacker groups and cybercriminal organisations—resulting in more harm than good.

6. Conclusion

The practice of mass surveillance against citizens all over the world has never proven sufficient, if at all effective, to proactively stop terrorist attacks or improve national security in any noticeable manner. And aside from the technical defects of Internet censorship, it is usually found to be abused more often than not for suppressing freedom of information.

Additionally, introducing backdoors in digital encryption systems would only mean putting us all at a greater risk of cybercriminal attacks.

Further, the right to privacy is a human necessity that cannot be dismissed or given up under any circumstances. It's time we stand together to protect our civil liberties and freedom, putting an end to all such unconstitutional acts of censorship and surveillance done by repressive authorities worldwide.

7. Bibliography

7.1. References

[1] "Senate debates." The OpenAustralia Foundation. 2007. http://www.openaustralia.org.au/senate/?gid=2007-05-09.170.3.

[2] "Transparency report." Twitter, Inc. 2014. https://transparency.twitter.com/en/removal-requests.html.

[3] Gao, George. "What Americans think about NSA surveillance, national security and privacy." Pew Research Center. 2015. http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/.

[4] "Global Internet User Survey." Internet Society. 2012. http://www.internetsociety.org/surveyexplorer/key_findings.

[5] Dennis, Everette E., Justin D. Martin, and Robb Wood. "Censorship, Regulation, Surveillance." Northwestern University in Qatar. 2016. http://www.mideastmedia.org/survey/2016/chapter/censorship-regulation-and-online-surveillance/.

[6] Cahall, Bailey, Peter Bergen, David Sterman, and Emily Schneider. New America. 2014. https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/.

[7] "Voting results of the surveillance system." 2016. http://vote.duma.gov.ru/vote/94599.

[8] "Australia secretly censors Wikileaks press release and Danish Internet censorship list." 2009. https://wikileaks.org/wiki/Australia_secretly_censors_Wikileaks_press_release_and_Danish_Internet_censorship_list,_16_Mar_2009.

[9] Shaheen, Kareem. "Turkey blocks access to WikiLeaks after Erdogan party emails go online." The Guardian. 2016. https://www.theguardian.com/world/2016/jul/20/turkey-blocks-access-to-wikileaks-after-erdogan-party-emails-go-online.

[10] Taylor and Francis. "Routledge handbook of Internet politics." (2010): 323–324.

[11] McCullagh, Declan. "Google's chastity belt too tight." CNET News. 2004. https://www.cnet.com/news/googles-chastity-belt-too-tight/.

[12] Jalon, Allan M. "A break-in to end all break-ins." Los Angeles Times. 2006. http://articles.latimes.com/2006/mar/08/opinion/oe-jalon8.

[*] "Cyber Security and Online Citizenship in MENA." Fanack Academy. 2016. https://academy.fanack.com/publications/2016/09/15/essay-contest-on-cyber-security-and-online-citizenship/.