Ulises Maldonado

Margaret Shannon

English 3

3 December 2019

Americanize, Americanize: View the World from American Eyes

Considering the fact that 58% of global cloud infrastructure services are hosted by four American companies (Synergy Research Group 2017), it is no wonder the Trump Administration is regurgitating the mandate for a backdoor on encryption. If congress passes any bill that requires American companies to comply with such an order, the United States would have access to more than half of the world's private information. Such a bill would bring unpronounced consequences that the general public and Congress do not understand. Allowing tech illiterate congresspeople decide how we should protect our private information will lead to exploitation from government agencies in the name of "security". Although the United States government wants us to believe requiring a backdoor for encryption is a necessity for national security, their track record should be a warning for us to view this as a hidden attempt to regain control over their citizens' private communications.

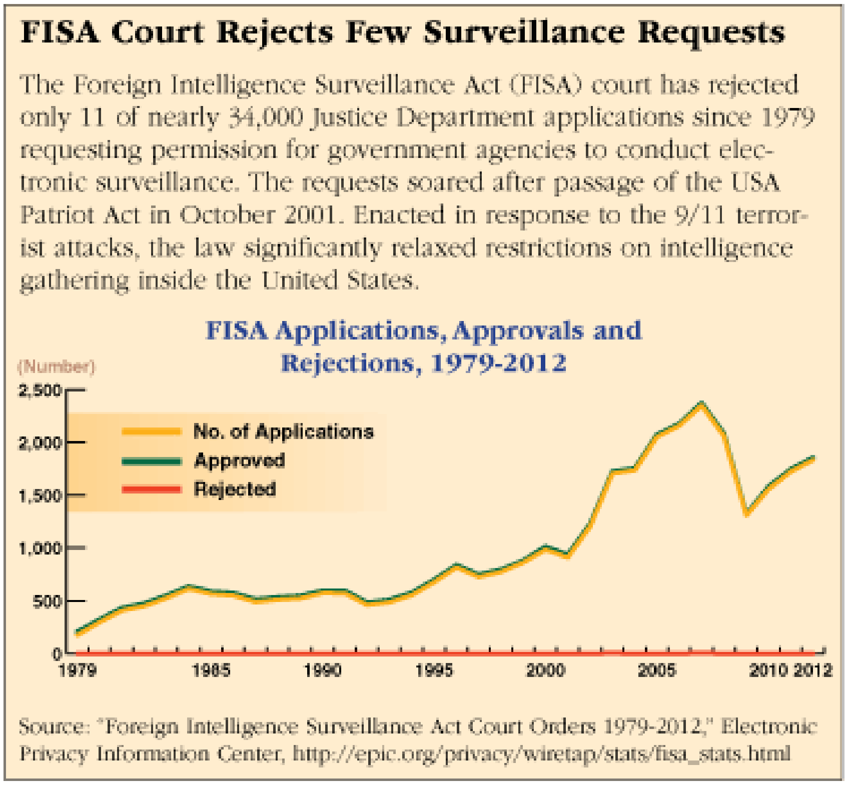
The terrible track record of the United States should be emphasized because it shows the importance behind why we can not trust them. For instance, leaked documents from Edward Snowden, a former NSA contractor, show the NSA purposely created a flawed encryption formula and paid RSA, a security firm, $10 million to use the formula as the default for encryption (Menn 2013). This gave the NSA a personal backdoor to anyone or any company using the flawed encryption formula. Of course, the NSA denies this claim. In addition to that, Snowden exposed the existence of PRISM, a surveillance program that collects information about users from companies such as Google, Microsoft, and Facebook in exchange for immunity. However, the government is much more open about this program. They claim the mass surveillance is “narrow” in focus and has saved lives (Madison 2013). We already know they have tried and succeeded in exploiting any loophole they can find (or integrate), so what is saying this push toward requiring a backdoor is not going to meet the same fate and be used for mass surveillance? These two examples from Snowden alone show how desperate the government is to gain access to their citizens’ personal information and communications.

But is the government *really* trying to regain control over their citizens? Yes, it seems so, and Thomas Friedman, a *New York Times* columnist and Pulitzer Prize winner, brings up a good point in his book, *Longitudes and Attitudes: The World in the Age of Terrorism*. Friedman states, “Individuals can increasingly act on the world stage directly, *unmediated by a state* (emphasis added)” (Friedman, *Longitudes and Attitudes* 5). In other words, Friedman believes the individual, independent of government, can accomplish tasks that used to be reserved for government and its agencies. This is all thanks to the power of the Internet for communication. That explains why the government is fearful of encryption; they are fearful of losing control of tasks that they deem should be reserved for them. If companies encrypt all communications, individuals could do as they please which might include protests, organizations, or give a speech at the UN about how horrible their country is regarding climate change, without their government being able to snoop on them until the event is ongoing. On the other hand, if backdoors on encryption are mandated, the government will simply use them to stop anything or anyone that threatens their power. Is someone planning a peaceful protest because a congressperson did something unlawful? Sorry buddy, we are shutting it down ahead of time to prevent “riots”. So, the question really is not *is the government trying to regain control over their* *citizens*, the question is *how far is the government willing to go to regain control over their citizens*?

What the government does not seem to realize is that building a backdoor for a single entity is a huge task to accomplish and also a greater security risk. It is foolish to believe that there is a way to allow access to the “good guys” without expecting for it to fall into the hands of the “bad guys”. In essence, the government, if they choose to proceed with a backdoor requirement, would be opening up a doorway for any bad actor who happens to acquire a decryption “key” in return for unlimited 24/7 access to encrypted data. However, do not just take my word for it; researchers from MIT published a report, “Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications,” that goes into detail about the dangers of giving law enforcement and government agencies a “key that [guarantees] access to everything”. These researchers, who have been arguing *against* backdoors for encryption since the 80s and 90s, also go on to say that the government requesting these backdoors does not really grasp the severity of what they are asking for. They summarize by asserting, “The costs [to implement a backdoor] would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict” (Abelson, et al. 2015). And, we do not even need to go far to understand the disastrous effects of giving people a “key” that has access to everything. Take the OPM (Office of Personnel Management) data breach for example; a government agency suffered a data breach because they allowed contractors “free access to [their] system,” a backdoor, if you will (Fruhlinger 2018). Chinese counterintelligence hackers then exploited this backdoor to extract personal information from millions of federal employees. This is a hyperlocalized example of a backdoor being used in unintended ways. What is saying history is not going to repeat itself if the government mandates a backdoor on encryption?

Of course, the general public may object to my claims that the United States government is trying to regain control over citizens private communications. They most likely believe that the government is doing this in their best interest, for national security. I can not really fault them for believing it either because the United States government has done a great job of advertising their actions as such. A recent example of this would be an open letter addressed to Mark Zuckerberg from the United Kingdom Secretary of State for the Home Department, United States Attorney General, United States Secretary of Homeland Security, and Australian Minister for Home Affairs. In this open letter, titled "Facebook's 'Privacy First' Proposals," these governments express their support for encryption; however, they only support it *if* they are allowed access to a backdoor (Patel, Barr, McAleenan, & Dutton 2019). Their reasoning is that they must have a way to prevent crimes manifesting online from leaking into the "physical world". In this letter, they focus on Facebook's efforts to fight child exploitation and claim encryption, without a backdoor, would encourage these actions. However, after appealing to emotion, they make sure to note that Facebook should cooperate with law enforcement to "[obtain] the content of communications, under appropriate legal authorization, to save lives, enable criminals to be brought to justice, and exonerate the innocent," revealing their true motive behind the letter. They know they must win over the general public, so they include a sob story before getting to their demands. This way, the general public considers the demands as reasonable because they are in the name of "national security". Perhaps at times, some of these demands are reasonable, but most of the time they are not. In Thomas Friedman's book, *The World Is Flat: A Brief History of the Twenty-First Century*, he argues "The playing field is not being leveled only in ways that draw in and superempower a whole new group of innovators. It's being leveled in a way that draws in and superempowers a whole new group of angry, frustrated, and humiliated men and women" (Friedman, *The World is Flat*). In making this argument, Friedman contends that advancements in technology and education have gradually made us more equal; however, an unwanted side effect is our enemies are also the ones benefiting from those advancements. While we do have terrorists using encryption, and we do have terrorists using encrypted messaging services, is that really a good enough reason to spy on everyone? Is the government demanding companies to have a backdoor to *possibly* prevent terrorist attacks worth the breach of privacy to millions of lawful citizens?

It is evidentially clear that encryption would stop the government from easily, and illegally, spying on regular citizens whom they deem as a "possible risk". We see this in information gathered from Foreign Intelligence Surveillance Act (FISA) requests. FISA's purpose was to stop the illegal and rampant surveillance that was being conducted by federal agencies in the 20th century ("Domestic Surveillance;" "Select Committee to Study Governmental Operations"). However, that did not stop the surveillance; it was simply a roadblock that accomplished



FISA Court Rejects Few Surveillance Requests

The Foreign Intelligence Surveillance Act (FISA) court has rejected only 11 of nearly 34,000 Justice Department applications since 1979 requesting permission for government agencies to conduct electronic surveillance. The requests soared after passage of the USA Patriot Act in October 2001. Enacted in response to the 9/11 terrorist attacks, the law significantly relaxed restrictions on intelligence gathering inside the United States.

Source: "Foreign Intelligence Surveillance Act Court Orders 1979-2012," Electronic Privacy Information Center, http://epic.org/privacy/wiretap/stats/fisa_stats.html

Figure 1 ("Foreign Intelligence Surveillance Act Court Orders") nothing as shown in *Figure 1* ("Foreign Intelligence Surveillance Act Court Orders"). The FISA court, which reviews FISA requests, has only denied 11 requests out of 34,000 from 1979-2012. That means that 33,989 requests to spy on an individual, or an organization, were permitted leaving you to wonder how many false positives occurred. Individuals should have the right to protect themselves against unfair and unjust surveillance from governmental agencies who seem to have no checks and balances in place. The only plausible solution is to encrypt your data and communications. With encryption, lawful citizens can do their day-to-day tasks without worrying if the government is listening in.

Encryption might only be a bandage for an inevitable problem, however. A report from *Wired* titled, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," details the construction of a "spy center" which will be "five times the size of the US Capitol" once built (Banford). This $2 billion center, which is now built, serves multiple purposes, and one of those purposes is cracking encryption. In fact, since the construction of this center, the NSA has cracked a couple of encryption methods thanks to their supercomputers (Hern). There is reason to worry thanks to this center and many others constructed around the United States. *Figure 2* shows how the main Utah Data Center, which is

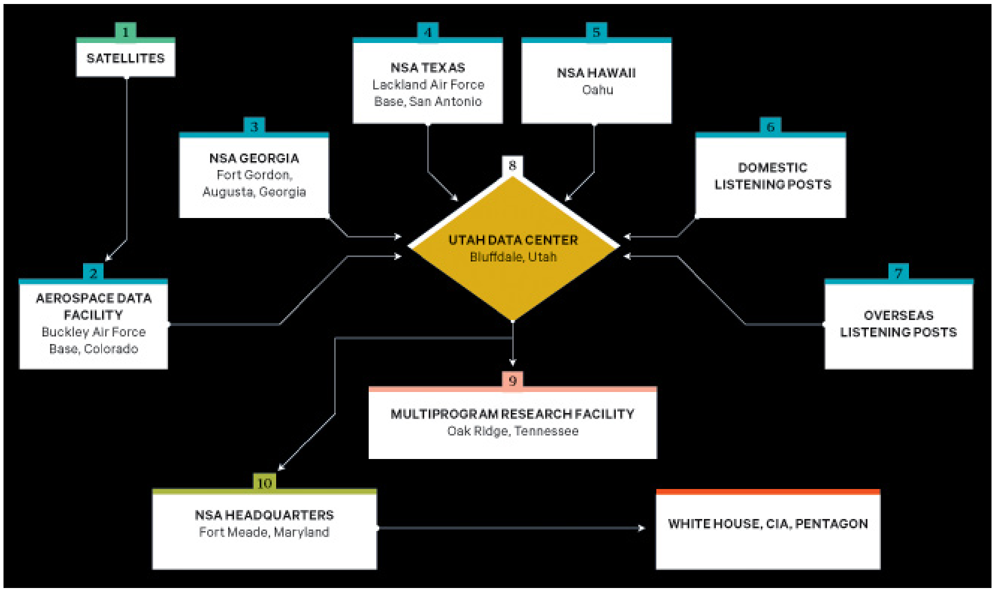
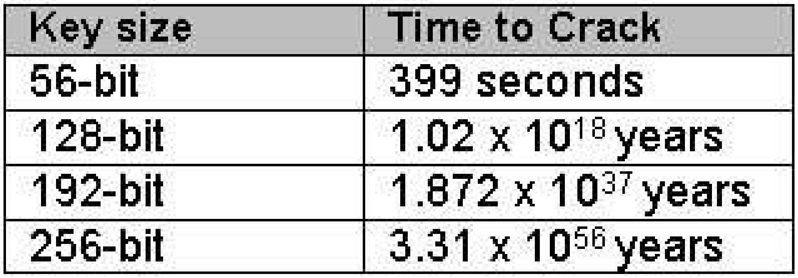


Figure 2 (Bamford)

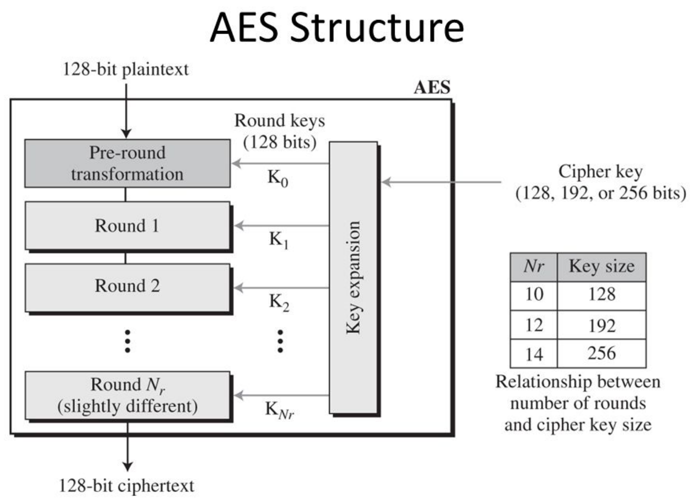
the $2 billion center, is the main hub for several agencies and sources of communication (Bamford). If there is any encrypted data that proves to be challenging for other governmental agencies, they use the processing power available from the center to try and crack it. With a post 9/11 almost blank check, the NSA is a force to be reckoned with and one that many researchers and activists are trying to slow down.

On the upside of the NSA cracking encryption, researchers are working on something better: stronger encryption. Encryption is exponential, meaning the longer the security key, the longer it will take to try and crack the encryption key. For instance, one of the popular encryption methods is Advanced Encryption Standard (AES) and it comes in three different flavors, 128 bits, 192 bits, and 256 bits. According to Mohit Arora, a researcher and semiconductor engineer, the "weakest" version, 128 bits, would take 1 billion billion years to crack if using a brute force method, as shown in *Figure 3* (Arora). That's not a mistake, the number is quite hard to represent so the best manner to represent it is simply by saying "1 billion *billion*" years. So, the "weakest" version would take longer to crack than the age of the universe. With 192 bits and 256 bits, it's almost theoretical impossible to measure the amount of time needed to crack these versions. That's great isn't it? What are we worried about if it's almost impossible to brute force these encryption methods? The keen of you will notice that "brute force" is mentioned often. That is because brute forcing is not the only method of breaking encryption, there are several other methods. Malwarebytes Labs, a security research company, details the structure of the AES encryption standard and the various



Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Figure 3 (Arora)



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Figure 4 (Hioureas)

attack surfaces that can be targeted. As you can see in *Figure 4*, you can target the inputs such as the plaintext, the data being entered before encryption, or the cipher key, the encryption key used to “scramble” the data and encrypt it (Hioureas). This is what we fear from the NSA and the remaining federal agencies. They know where to focus their research and attacks on and we are allowing them to do so by ignoring their blatant attempts of undermining out rights.

While there are many complexities to encryption, at the end of the day, we can only hope both sides want what is best for everyone. We, however, can not allow a government who is unable to cite a specific incident that was successfully prevented using *unencrypted* data on a phone to tell us this is a necessity (Froomkin & Vargas-Cooper 2014). If it were to be a necessity, then there would be evidence that would show how data stored on a phone could help prevent crimes. If government and its agencies can not pull any useful information out of *unencrypted* phones, which is the main medium for communication, we can infer this is a poor excuse for mass surveillance. Government as a whole is already incredibly powerful, way more powerful than intended. Why should we be compliant to their unjust attempts to gain illicit power over us and our everyday lives and communications? It is not often we see big tech companies fighting for our rights, and we should always be skeptical when they are, but privacy should always be the number one concern for any company and for our own government.

Works Cited

Abelson, Harold M., et al. “Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications.” *MIT Libraries*, 7 July 2015, https://dspace.mit.edu/handle/1721.1/97690.

Arora, Mohit. “How Secure Is AES against Brute Force Attacks?” *EETimes*, EE Times, 7 May 2012, www.eetimes.com/document.asp?doc_id=1279619.

Bamford, James. “The NSA Is Building the Country's Biggest Spy Center (Watch What You Say).” *Wired*, Conde Nasté, 7 Mar. 2018, www.wired.com/2012/03/ff-nsadatacenter/.

"Domestic Surveillance." *Gale Opposing Viewpoints Online Collection*, Gale, 2019. *Gale In Context: Opposing Viewpoints*, https://link.gale.com/apps/doc/PC3021900130/OVIC?u=cclc_lbcc&sid=OVIC&xid=72df66ed. Accessed 18 Nov. 2019.

“Foreign Intelligence Surveillance Act Court Orders 1979-2017.” *Electronic Privacy Information Center*, epic.org/privacy/surveillance/fisa/stats/default.html.

Friedman, Thomas L. “Prologue.” *Longitudes and Attitudes: The World in the Age of Terrorism,* Anchor, 2003, p. 5.

Friedman, Thomas L. “Introduction.” *The World Is Flat: A Brief History of the Twenty-First Century*, Farrar, Straus and Giroux, 2005.

Froomkin, Dan, and Natasha Vargas-Cooper. “The FBI Director's Evidence Against Encryption Is Pathetic.” *The Intercept*, 17 Oct. 2014, https://theintercept.com/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb.

Fruhlinger, Josh. “The OPM Hack Explained: Bad Security Practices Meet China's Captain America.” *CSO Online*, CSO, 6 Nov. 2018, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Harwood, Matthew, and Hina Shamsi. “How Surveillance Turns Ordinary People Into Terrorism Suspects.” *Mother Jones*, 6 Nov. 2014, www.motherjones.com/politics/2014/11/how-surveillance-turns-ordinary-people-terrorism-suspects/.

Hern, Alex. “The NSA May Have Been Able to Crack so Much Encryption Thanks to a Simple Mistake.” *Business Insider*, Business Insider, 16 Oct. 2015, www.businessinsider.com/nsa-able-to-crack-encryption-thanks-to-a-simple-mistake-2015-10.

Hioureas, Vasilios. “Encryption 101: How to Break Encryption.” *Malwarebytes Labs*, Malwarebytes, 22 Mar. 2018, blog.malwarebytes.com/threat-analysis/2018/03/encryption-101-how-to-break-encryption/.

Madison, Lucy. “Obama Defends ‘Narrow’ Surveillance Programs.” *CBS News*, CBS Interactive, 19 June 2013, https://www.cbsnews.com/news/obama-defends-narrow-surveillance-programs.

Menn, Joseph. “Exclusive: Secret Contract Tied NSA and Security Industry Pioneer.” *Reuters*, 20 Dec. 2013, www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220.

Patel, Priti, et al. “OPEN LETTER: FACEBOOK’S ‘PRIVACY FIRST’ PROPOSALS.” *The United States Department of Justice*, 4 Oct. 2019, https://www.justice.gov/opa/press-release/file/1207081.

Select Committee to Study Governmental Operations with Respect to Intelligence Activities. United States Senate, www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm. Accessed 18 Nov. 2019.

Synergy Research Group. “The Leading Cloud Providers Continue to Run Away with the Market.” *Synergy Research Group*, 27 July 2017, https://www.srgresearch.com/articles/leading-cloud-providers-continue-run-away-market.