The End of Information Privacy and Security: Encryption Backdoors

Chelsea Zimmerman

School of Government, Liberty University

Author Note:

Disclosure: I work for a cybersecurity company and therefore have a favorable bias toward encryption integrity and security. I also have first-hand knowledge of organizations being victimized by ransomware and other cyber attacks.

Contact information regarding this paper should go to the following email: czimmerman1@liberty.edu

ABSTRACT

In an effort to combat child exploitation crimes, terrorism, and other criminal acts, the United States government (as well as several foreign governments) has called on technology companies to build "backdoors" into their platforms, applications, and devices so law enforcement can circumvent proprietary encryption coding. The primary problem right now is end-to-end encryption of these platforms, applications, and devices which prevents law enforcement from accessing digital evidence – sometimes even if they have a warrant. While encryption backdoors would facilitate the speedy recovery of digital evidence for law enforcement, it opens up a can of worms in other areas. Current literature and discussion around encryption backdoors reveal there is a gap in the research in terms of principle and technical restraints. The author holds private companies engaged in commerce within the borders of the United States should not be compelled to provide "back doors" to law enforcement to circumvent proprietary encryption coding because it makes the people and the nation less secure.

Keywords: encryption backdoor; end-to-end encryption; digital evidence; SolarWinds

Introduction

In 2020, digital devices and cloud storage hold more private details of a person's life than a traditional diary ever could: every message, every photo, every "like," every association. For a law enforcement officer investigating a crime, this kind of data is a digital treasure trove of potential evidence. However, modern-day encryption makes this data inaccessible to law enforcement. In an effort to combat child exploitation crimes, terrorism, and other criminal acts, the United States government (as well as several foreign governments) has called on technology companies to build "backdoors" into their platforms, applications, and devices for law enforcement to circumvent proprietary encryption coding.

There are three major arguments against encryption backdoors for law enforcement: (1) this level of unfiltered government surveillance infringes on individuals' Fourth Amendment rights to be secure in their property; (2) encryption backdoors are a principle problem because they could be exploited by criminals and foreign nations; (3) encryption backdoors are a technical problem since they are not mathematically possible. While there is much literature surrounding the first argument, less discussion has taken place around the second and third arguments. After examination, this author finds private companies engaged in commerce within the borders of the United States should not be compelled to provide "back doors" to law enforcement to circumvent proprietary encryption coding, because it makes the people and the nation less secure.

Background

End-to-end encryption is a data security technique that uses cryptology and applied math. A data set is "encrypted" by jumbling the information into an unreadable format while it is in transit. When the data reaches its intended destination, a shared key is used to "decrypt" the data, making it readable once again. Without the key, the encrypted data cannot be read. Tom Scott (2017) says to look at encryption like a complicated math problem: if you multiply two prime numbers together you get a quotient quickly. However, if you were to try to reverse engineer the math problem to try and figure out what two numbers you would need to multiply to get that quotient, the answer will take much longer to figure out. This is like decrypting. Scott says "modern cryptography uses way more complicated one-way operations. . . . you can have a computer do math that is simple one way but could take longer than the lifetime of the universe to brute-force back" (Scott, 2017). This explains why the FBI and other government officials and agencies want a backdoor to encryption; there is no way for them to access encrypted information unless the user willingly unlocks it.

The solution Attorney General Barr and other government officials have come up with is to create legislation that mandates technology companies to build "backdoors" into their devices and systems to circumvent the encryption coding. Scott compares backdoors to a convential way police already gather electronic information – wiretaps. "Backdoors have been allowed for old-school phone conversations for decades – they're called wiretaps," Scott explains, continuing, "It's called a wiretap because many years ago the police would literally be attaching a device to a physical phone wire. So for anyone who grew up knowing that, anyone who grew up with [old, boxy] computers – like pretty much every politician in government – well, it seems reasonable that should also extend to, for example, WhatsApp" (Scott, 2017). WhatsApp is the encrypted global messaging platform owned by Facebook. Scott alludes to the idea that many lawmakers do not understand the leaps that have happened with technology and the implications of those leaps. If wiretaps are fine, why are encryption backdoors any different – they both reveal to police information that would not normally be accessible to anyone other than the participants of the data exchange.

Wiretaps are governed by The Wiretap Statute, 18 U.S.C. §§2510-22, which "regulates the interception of the contents of wire, oral, or electronic communications, that is, 'real-time' capture of the communications in transit" (Clancy, 2019, p. 388). Wiretaps can only be conducted by the government when a wiretap order is issued by a federal court and law enforcement has probable cause, similar to the process for a warrant. The wiretap order can only be issued once all other "investigative procedures have been tried and failed" or shown "unlikely to succeed if tried or to be too dangerous" (18 U.S.C. §2518(1)(c)).

In comparison, backdoors for encryption allow law enforcement to bypass the encryption coding and retrieve any content they desire, both real-time data in transit and retrospective stored data. Currently, the legal way to obtain stored communications is through the Stored Communications Act (SCA), 18 U.S.C. §§2701-12. This legislation was created to regulate the disclosure of stored communication content by third-party electronic communication services and remote computing services (Clancy, 2019, p. 395). Compelled disclosures through the SCA "need a search warrant, a 2703(d) court order, or a subpoena," similar to the Wiretap Act (Clancy, 2019, p. 397).

The Problems

Fourth Amendment Applicability

The Fourth Amendment gives people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government (U.S. Const. amend. IV). For information to be protected under the Fourth Amendment, it must be considered a protected interest, which is “defined by the Supreme Court as a reasonable expectation of privacy in the data sought” (Clancy, 2019, p. 293). In *Riley v. California* (2014) the Court observed: “The fact that technology now allows an individual to carry such [private] information in the palm of his hand does not make the information any less worthy of the protection for which the founders fought” (*Riley v. California*, 2014, Oral Opinion, 8:18). Building on this decision, the Court in *Carpenter v. United States* (2018) found cell-site location information to be a protected interest that requires a warrant to search and seize. The Court applied *Katz v. United States* (1957), saying “a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years” would be an invasion of a person’s reasonable expectation of privacy (*Carpenter v. United States*, 2018).

The decision in *Carpenter* has reaching conclusions. Although the Court declined to explicitly extend this decision to other types of stored data for the time being, the informal definition of encrypted data (like email, messages, device application data, etc.) could arguably be “a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years” (*Carpenter v. United States*, 2018). If this is true, law enforcement would need to obtain a warrant to search and seize encrypted data.

The Fourth Amendment only considers searches and seizures by the government; it does not consider searches and seizures by criminals, foreign actors, and terrorists. This is why encryption backdoors are not purely a Fourth Amendment problem.

Not Principally Possible

In January, 2020, President Trump and Attorney General Barr requested Apple to unlock the phones of an alleged shooter so the FBI could look for digital evidence. Because the phones used end-to-end encryption, the FBI could not access the data inside without an encryption key.

This type of situation is why the government is calling for “backdoors” for law enforcement to get around Apple’s and other manufacturers’ devices’ propriety encryption coding. Although Apple is willing to help law enforcement in other ways, such as turning over data from its servers, they are against building backdoors to circumvent their encryption; they are also against unlocking their customers’ devices for law enforcement (Leswing, 2020). It is not just Apple that feels this way.

Previous to the request to Apple, Attorney General Barr along with the then acting Secretary of Homeland Security, United Kingdom Secretary of State for the Home Department, and the Australian Minister for Home Affairs, wrote to Facebook’s CEO Mark Zuckerberg in an open letter asking for an encryption backdoor for their proprietary coding. The letter requested that Facebook and its sister companies “[e]nable law enforcement to obtain lawful access to content in a readable and usable format” (Barr et al. to Facebook, October 4, 2019, p. 3). A “readable and usable format” means decrypted. In response, Facebook wrote back “The ‘backdoor’ access you are demanding for law enforcement would be a gift to criminals, hackers and repressive regimes, creating a way for them to enter our systems and leaving every person on our platforms more vulnerable to real-life harm. It is simply impossible to create such a backdoor for one purpose and not expect others to try and open it” (Facebook to Barr et al., December 29, 2019, p. 1). Once the door is unlocked for one person it is unlocked for everyone; this is why backdoors are not principally possible.

Not Technically Possible

As of the time of this writing, the only person who can unlock an encrypted device or platform is the user. Not even the tech companies who created these platforms can unlock the encrypted data. This is the modern standard for privacy and security. The encrypted data could be useful to law enforcement during an investigation, however they do not have access to it currently. Scott explains that with encryption in place, “if any [third party apps like WhatsApp or iMessage] get served with a government warrant right now, the most they could do is say how much two people have been talking and maybe roughly where they were – but never what they were talking about. More than that is literally mathematically impossible” (Scott, 2017). Requiring tech companies to create a backdoor to circumvent the encryption is not like creating a spare key; It is like smashing the glass in the window to reach in and unlock the door from the inside.

As described earlier, end-to-end encryption creates a lock that is so strong, there is no mathematically possible way to reverse-engineer it. The only way to get a “backdoor” is to intentionally design the device or platform with a vulnerability. Vulnerabilities can be exploited by anyone that finds them, so it is technically impossible to make a backdoor with only one key.

Review of Literature

Why is Encryption the Standard?

When the NSA whistleblower Edward Snowden revealed in 2013 that the American government was “routinely spy[ing]” on its citizens, he brought the attention of the public to data privacy and the use of encryption (The New American, 2018). Popular messaging services like WhatsApp and iMessage started encrypting their platforms and companies like Apple introduced end-to-end encryption for their devices. The language these companies used to advertise their products started to change, focusing on the privacy users wanted in communications. WhatsApp’s security page now reads, “Some of your most personal moments are shared with WhatsApp, which is why we built end-to-end encryption into our app. . . . [¶] End-to-end encryption ensures only you and the person you're communicating with can read or listen to what is sent, and nobody in between, not even WhatsApp” (WhatsApp, 2020). Similarly, Apple tells its customers, “Privacy is built in from the beginning. Our products and features include innovative privacy technologies and techniques designed to minimize how much of your data we — or anyone else — can access. And powerful security features help prevent anyone except you from being able to access your information. We are constantly working on new ways to keep your personal information safe" (Apple, 2020). Clearly, Americans choose encryption as the standard because they value their privacy, but encryption is also vital for national security.

Unintended Consequences

One of the "worst case[s] of ransomware comes from an NSA exploited backdoor inside of the Windows operating system" (Swann, 2019). The attack was aptly called WannaCry, and according to *The New York Times*, "The tool was leaked by a group calling itself the Shadow Brokers, which ha[d] been dumping stolen NSA hacking tools online since [2016]. Microsoft rolled out a patch for the vulnerability in March [2017], but hackers apparently took advantage of the fact that vulnerable targets — particularly hospitals — had yet to update their systems or had ignored advisories from Microsoft to do so" (Bilefsky, 2017). This is an unintended consequence of encryption backdoors.

At the time of this writing, the nation is still trying to understand an eerily similar case taking place. The "SUNBURST backdoor" for SolarWind's Orion software was exploited in December 2020, allowing a hacking group to penetrate the systems of (at least) the departments of State, Homeland Security, Commerce, and Treasury, and the National Institutes of Health (Kaplan, 2020). It could come to light that more departments were hit, as "[o]n its website, SolarWinds says it has 300,000 customers worldwide, including all five branches of the U.S. military, the Pentagon, the State Department, NASA, the National Security Agency, the Department of Justice and the White House. It says the 10 leading U.S. telecommunications companies and top five U.S.

accounting firms are among customers" (Tucker et al., 2020). Besides the obvious concerns of the hack, it is important to note that the attackers first gained entry to the SolarWinds system in March, 2020, which means the communications and data of government officials could have been compromised for months without their knowledge (Tucker et al., 2020). Also alarming to national security, SolarWinds is the company behind Serv-U, the file transfer program used by the Dominion voting machines in the 2020 presidential election (White, 2020). It is possible this program could have been affected by the hack, as software companies tend to share code between their different products and division teams.

The cybersecurity company FireEye was also hacked through the Orion software vulnerability and in the process, all of its hacking tools were stolen (Tucker et al., 2020). The fallout from this is still unknown, as new attacks using these tools could soon surface.

Solution

Because of The Stored Communications Act, companies and people are aware that information can be subpoenaed or searched with a warrant obtained with probable cause. It is then unnecessary to create backdoors that would provide unlimited access to peoples' encrypted devices and platforms when there are other options to retrieve the data. Encrypted data can be considered a locked container, and like other locked containers, it should be searched with a proper warrant.

The Gap in the Research

There is already sound discussion about how government access to encrypted data is harmful to individuals and may breach the Fourth Amendment. What is lacking in the discussion is the effects on national security. National security is threatened by encryption backdoors. Just looking at the national security issues WannaCry and the SUNBURST backdoor created, researchers can see encryption backdoors are a bigger problem than they are a solution. Backdoors are vulnerabilities purposely made to bypass encryption, leaving the people of the United States, critical infrastructure, and government secrets exposed to criminal actors, terrorists, and foreign nations.

Cyber criminals are not hooded nerds in their moms' basements. They are sophisticated, weaponized criminal enterprises backed by nation-state sponsors. They have CEOs, CFOs, and organizational structure. Their full-time job is hacking, and they are good at it. Unfortunately, American businesses are often the target of their ransomware schemes, and if owners pay the ransom, they are often funding physical terrorism without realizing it (Department of Treasury, 2020). These business owners are then investigated to find out if they were negligent in their IT security, and if they did everything in their power to prevent such an attack. If the answer is no, they are held liable and must pay huge fines – that is on top of the embarrassment in the media they will endure.

The hard part about this is "there is no nomenclature for cyber risk. It is not like an earthquake or hurricane that is measured in magnitude or knots" (The CyberCall, 2020). There is no way to tell what the damage will be when Sandy the receptionist clicks on a phishing link in an email. In today's threat landscape it is impossible to completely prevent a cyber attack, even if individuals and businesses are doing everything in their power to secure their technology environment. Malware is evolving so rapidly, cybersecurity specialists are habitually "playing Bingo not blackout" (The CyberCall, 2020).

Cyber criminals pick on those that are "the least prepared and most vulnerable" (The CyberCall, 2020). The best way to protect the nation from cyber attacks is to look at cybersecurity from a layered approach. Encryption is the best defense against cyber attacks but, by its design, only works if it is impenetrable. Backdoors dissolve the value of the encryption.

The Opposition

Third Party Doctrine

Third Party doctrine is the idea that if someone willingly gives their information over to a third party they have no protected interest in it. Justice Altio, dissenting in *Carpenter v. United States* (2018) wrote, "As the Court well knows, the reason that we have never seen such a case is because – until today – defendants categorically had no "reasonable expectation of privacy" and no property interests in records belonging to third parties" (*Carpenter v. United States*, 2018, Alito, J., dissenting, p. 17). Since the cell-site data in this case was held by the phone company, Third Party doctrine would normally hold the defendant did not own the data but instead the phone company did. Justice Kennedy added in his dissent, "the government did not search anything over which Carpenter could assert ownership or control. Instead, it issued a court-authorized subpoena to a third party to disclose information it alone owned and controlled" (*Carpenter v. United States*, 2018, Kennedy, J., dissenting, p. 22). If Third Party doctrine would have been applied to this case, the Fourth Amendment would have offered no protection.

When applying *Carpenter* to cloud computing and encrypted data, Justice Gorsuch's dissent is helpful: "At least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern life, and in that way the fact that we store data with third parties may amount to a sort of involuntary bailment too" (*Carpenter v. United States*, 2018, Gorsuch, J., dissenting, p. 17). Many times it is not a choice for people to turn over their data to cloud providers because of the necessity of offsite storage and backups. Justice Gorsuch is saying that Fourth Amendment protection could be extended to data in the cloud if that data is seen as a bailment – someone holding your stuff for you. "It seems entirely possible a person's cell-site data could qualify as his papers or effects under existing law. Yes, the telephone carrier holds the information. But. . . [p]lainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right" (*Carpenter v. United States*, 2018, Gorsuch, J., dissenting, pp. 20-21). The debate is sure to continue in the future on whether or not encrypted data is considered a protected interest or Third Party data.

The Push for Legislation

Attorney General Barr and other international ministers released a press release through the Department of Justice in October 2020. It called for backdoors to companies' proprietary end-to-end encryption for law enforcement, citing its main reason as the explosion of child exploitation in the digital era. The statement says, "measures to increase privacy – including end-to-end encryption – should not come at the expense of children's safety" (US Department of Justice, Office of Public Affairs, 2020). Because child pornographers are increasingly using encryption to protect the privacy of their data, it is becoming cumbersome for law enforcement to obtain digital evidence of the crime swiftly.

Right now there is an attempt being made at legislation to enforce Attorney General Barr's desire for encryption backdoors. The Lawful Access to Encrypted Data Act Bill, S. 4051, is in the Senate at the time of this writing. The Act, if passed, would require technology companies to build backdoors into their devices and platforms to comply with warrant requirements: "Once a warrant is obtained, the bill would require device manufacturers and service providers to assist law enforcement with accessing encrypted data if assistance would aid in the execution of the warrant" (Committee on the Judiciary, 2020). Such data can only be obtained through a backdoor because that is the only way to get through the encryption.

This author does not discount the value of encrypted evidence to the judicial system; however, "[one] cannot let the cure be worse than the problem itself" (Trump, 2020). Based on the privacy issues and the national security problems encryption backdoors would face, they should not be considered a viable option to combat crime. Even if the Supreme Court one day held that Third Party doctrine applied to encrypted data, the other two arguments of principal and practical impossibility would render the argument of Fourth Amendment applicability moot.

Implications of Encryption Backdoors

Jeff Hudson, CEO of Venafi, spoke of the implications for encryption backdoors when it comes to national infrastructure:

> What's trying to happen here is control – control of the people, ability to see everything – but the cost of that control is that we're not going to be able to trust self-driving cars, which are on the internet; we're not going to be able to trust nuclear reactors which are hooked to the internet; we're not going to be able to trust airplanes which are on the internet. We're not going to be able to trust anything because first principles are that if there is a backdoor it will be exploited by people that were not intended to have access to that backdoor and it's a principle (and in practice, it's proven true a hundred percent of the time). If somebody is successful at putting backdoors in or getting encryption backdoors into technology all the things that are hooked into the internet that are near and dear to our hearts are going to be vulnerable to cyber attacks. (Venafi, 2019)

As the nation has seen how powerful backdoors have been in hacking American government agencies, including the Department of Homeland Security, one can imagine how destructive a similar hack would be on something like the power grid or a dam.

Conclusion

At the end of Nicholas Carr's book *The Big Switch* there is an epilogue entitled Flame and Filament. The short two and a half pages reflect on the technology the world has known in the past, and looks to the future for technology that is not here yet. Carr's eloquently described generational cycle of technology is both somber and beautiful:

> We're still attracted to the flame at the end of the wick. We light candles to set a romantic or calming mood, to mark a special occasion. We buy ornamental lamps that are crafted to look like candleholders with bulbs shaped as stylized flames. But we can no longer know what it was like when fire was the source of all light. The number of people who remember life before the arrival of Edison's bulb has dwindled to just a few, and when they go they'll take with them all remaining memory of that earlier, pre-electric world. The same will happen, sometime toward the end of this century, with the memory of the world that existed before the computer and the Internet became commonplace. We'll be the ones who bear it away.
>
> All technological change is generational change. The full power and consequence of a new technology are unleashed only when those who have grown up with it become adults and begin to push their outdated parents to the margins. As the older generations die, they take with them their knowledge of what was lost when the new technology arrived, and only the sense of what was gained remains. It's in this way that progress covers its tracks, perpetually refreshing the illusion that where we are is where we were meant to be. (Carr, 2013, pp. 232-233)

Attorney General Barr has been one of the key leaders in the fight for encryption backdoors, but he is retiring in late December 2020. What does this mean for encryption policy? Will the issue be dropped? Can it be dropped at this point? When looking at technology security concerns today, legislators and the courts must think of the future and how the decisions they make will affect the next generation. Perhaps this will be the last generation to experience information privacy. Perhaps the next nation will know nothing but a Surveillance State – certainly creating a backdoor for encryption that would allow the government unfiltered surveillance of its people has the potential to foster a surveillance state. It also has the potential to encourage cyber criminals and terrorists to find and exploit vulnerable backdoors of American companies, infrastructure, and government. Both of these scenarios make the people and the nation less secure.

References

Apple. (2020). Privacy features. Apple. https://www.apple.com/privacy/features/

Barr, W., McAleenan, K., Patel, P., and Dutton, P. to Facebook. (October 4, 2019). Correspondence. https://www.justice.gov/opa/press-release/file/1207081/download

Bilefsky, D. (2017). Hackers hit dozens of nations, exploiting stolen NSA tool. *The New York Times*. https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html

Carpenter v. United States, 505 U.S., 138 S. Ct. 2206 (2018).

Carr, N. (2013). *The big switch: Rewiring the world from Edison to Google*. Norton.

Clancy, T. K. (2019). *Cyber crime and digital evidence* (3rd ed.). Carolina Academic Press.

Committee on the Judiciary. (2020). Graham, Cotton, Blackburn introduce balanced solution to bolster national security, end use of warrant-proof encryption that shields criminal activity. Committee on the Judiciary. https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity

Department of the Treasury. (2020). Advisory on potential sanctions risks for facilitating ransomware payments. Department of the Treasury. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Facebook to Barr, W., McAleenan, K., Patel, P., and Dutton, P. (December 29, 2019). Correspondence. https://about.fb.com/wp-content/uploads/2019/12/Facebook-Response-to-Barr-Patel-Dutton-Wolf-.pdf

Kaplan, F. (2020). The wrong hack. Slate. https://slate.com/news-and-politics/2020/12/solarwinds-trump-hack-fireeye.html

Leswing, K. (2020). Apple’s fight with Trump and the Justice Department is about more than two iPhones. CNBC. https://www.cnbc.com/2020/01/16/apple-fbi-backdoor-battle-is-about-more-than-two-iphones.html

Riley v. California, 573 U.S. 373 (2014). Oral opinion. https://supreme.justia.com/cases/federal/us/573/373/

Scott, T. (2017, July 3). *Why the government shouldn't break WhatsApp*. [Video]. YouTube. https://www.youtube.com/watch?v=CINVwWHlzTY

Swann, B. 2019. AG Barr demands tech companies build backdoor in encryption for law enforcement. https://www.youtube.com/watch?v=KtHast8m76Y

The CyberCall. (2020). This is a private industry association the author belongs to.

The New American. (2018). “New FBI Director hints at backdoors for encryption.” *The New American,* 34(6). https://thenewamerican.com/new-fbi-director-hints-at-backdoors-for-encryption/

The Stored Communications Act, 18 U.S.C. §§2701-12.

The Wiretap Statute, 18 U.S.C. §§2510-22.

Trump, D. J. [@realDonaldTrump]. 2020, March 22. WE CANNOT LET THE CURE BE WORSE THAN THE PROBLEM ITSELF. AT THE END OF THE 15 DAY PERIOD, WE WILL MAKE A DECISION AS TO WHICH WAY WE WANT TO GO! [Tweet]. Twitter. https://twitter.com/realDonaldTrump/status/1241935285916782593?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1241935285916782593%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fthehill.com%2Fhomenews

%2Fadministration%2F488965-trump-hints-at-changes-to-restrictions-we-cant-let-the-cure-be-worse

Tucker, E., Bajak, F., and O'Brien, M. (2020). Austin-based SolarWinds among US agencies hacked in monthslong global cyberspying campaign. KVUE. https://www.kvue.com/article/news/local/austin-texas-solarwinds-us-govt-hack/269-a542ed56-2439-456e-84af-ab1301792974

U.S. Const. amend. IV.

US Department of Justice, Office of Public Affairs. (2020, October 11). *International statement: End-to-end encryption and public safety* [Press release]. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Venafi. (2019, September 24). *Encryption Backdoors | What it Means for Machines and Cybersecurity*. [Video]. YouTube. https://www.youtube.com/watch?v=JGBIYXMowyQ

WhatsApp. (2020). WhatsApp security. WhatsApp. https://www.whatsapp.com/security/

White, A. (2020). Confirmed: Dominion uses SolarWinds software, denies using software included in devastating attack. *National File*. https://nationalfile.com/confirmed-dominion-uses-solarwinds-software-denies-using-software-included-in-devastating-hack/