**Allowing Backdoor Access**

Paul Farri

School of Business, Liberty University

CSIS-320 B02: IS Hardware and Software

Professor Merrick Martin

June 23, 2022

Author’s Note

517 Augusta National Way, TN 37934

**Abstract**

Companies such as Microsoft, Google, Facebook, and Amazon each have a wide variety of applications and services in which any demographic of customers may purchase or download for free and utilize for their devices. As these companies have expanded in size and accessibility, the concerns of many users abroad regarding potential spying by different entities such as the companies themselves or federal government have greatly increased over the years. After various attempts have been made by the federal government to acquire the rights to access encrypted devices and users’ personal communications through company services with backdoor access, the question of ethics has consistently surfaced. This has led to the current debate in terms of whether or not the federal government should be allowed to have direct access to personal devices and services through backdoor access allowed by the major technology companies that provide the devices and services. While allowing such access to the federal government can pose a potential risk to the privacy and personal information of the customers, it can also create an environment in which crimes that were previously shielded by device encryption can be stopped more efficiently. This would help in creating a safer digital environment in which criminals will be less likely to successfully use smart devices and company services to get away with their crimes. However, it is always important to remember that there must be a balance between the federal government’s access and device encryption by the technology and service companies. There should be an established form of cooperation in which neither side would have more power than the other in deciding how much privacy the customers of the products would possess or how much access the federal government would have to the smart devices themselves in terms of cyber security. This would ensure that security can be increased to stop criminal activities at a more efficient rate while protecting the customer data.

**Allowing Backdoor Access**

**Introduction and Thesis Statement**

Security and personal privacy are important aspects to keep in mind when a customer or group of consumers use their personal smart device, or the free services downloaded from the company providing them. By having a secure digital environment free from leaks or illegal access, their personal information can be protected and their safety from hackers and malicious outlets can be maintained. However, too much security within these devices and services can unintentionally make it more difficult for law enforcement in America to track down and stop criminals that leave behind evidence on encrypted devices. In recent years, American government officials have been pressuring large and influential companies such Facebook to allow for the creation of backdoor inside their end-to-end encryption within their messaging services (Corrigan, 2019). If such a backdoor is created, it would pave the way for law enforcement to communications between users that would normally be very difficult to access due to encryption and other security measures keeping the device virtually shielded. Former Attorney General William Bar and former Homeland Security Acting Secretary Kevin McAleenan sent a letter to Facebook CEO Mark Zuckerberg stating that they would seek for Facebook to halt their plans on further encrypting Facebook’s messaging services until law enforcement would be able to unrestricted access to the messages within the service and ensure that user safety would not be reduced (Corrigan, 2019). In the year 2019 alone, twelve million reports of child abuse videos and imagery shared on Facebook Messenger was recovered by law enforcement. Despite concern for respecting of privacy and personal information of customers increasing, there has also been a large increase in criminal activity using encrypted devices and services over the last several years, the twelve million reports of child abuse material demonstrate a need for change.

**Allowing Backdoor Access**

**Ethics of Backdoor Access**

Companies such as Google, Facebook, Amazon, and Samsung allowing backdoor access to the federal government would face great amounts of concern from their respective customers and clients, as doing so would create a potential environment in which sensitive user data can be made easily accessible to the federal government. Each citizen in America is legally entitled to having the right to protect their personal data and information. If the federal government is granted access via backdoors inside smart devices and digital software services, that right could be violated for countless users of Samsung phones, Apple products, or even users of the Facebook application for their smart devices and pave the way for spying by government entities. As a result, the question of allowing backdoor access would raise many legal questions and debates.

In 2012, the FBI requested both Google and Facebook to provide reports for a wiretap backdoor. With backdoors built into Google and Facebook products, the FBI is able to conduct investigations through wiretapping. According to the report, the FBI would be required to receive a court order in order to proceed with the wiretapping, but this did not simmer concerns once the report became public. When the word had begun to spread of the report on the FBI using wiretap backdoors in popular web-based communication software and messaging services, it led to a noticeable outcry from users and internet freedom-advocating groups, who believe that it is a step towards the government regulating and monitoring the internet (eWeek, 2012). The report in question also stated that the FBI proposals would essentially be an amendment to the 1994 Communications Assistance for Law Enforcement Act. This would force Facebook, Twitter, Google, and other platforms to create FBI-accessible backdoors in their services.

This would also set the stage for the FBI being able to access data that would normally be acquired by Facebook directly from their users. For any type of interaction Facebook receives from any type of user, whether its in the form of a like on a page, making a follow request of an individual’s profile, that data is reported back to the company. This even applies for users that simply visit any page with a like button. Even if they did not make any further button inputs, that data is always transferred back to Facebook (eWeek, 2012).

In February of 2016, Apple CEO Tim Cook publicly announced to Apple product users across America that he was completely against an order from a federal court that required Apple to unlock an iPhone that the FBI, without exploring other options, wanted access to after the iPhone was discovered to have been used by one of the gunmen of the San Bernardino mass shooting in California, which took place in December 2015 (Zhang, 2016). The case the FBI had made against Apple was later dropped when the FBI found a third-party company that offered to sell them one of their tools to help them break into the shooter’s iPhone without Apple’s involvement. This is just one of the many cases across the country throughout the years in which the FBI has attempted to break into phones used by suspects of crimes. In 2017 alone, the FBI reported that they attempted yet failed to break into 7,800 locked phones and devices. After Mark Zuckerberg testified in April 2018, there were renewed calls by federal lawmakers in Washington D.C. for the regulation of large media companies like Facebook (Marks, 2018).

These examples demonstrate that despite the potential security benefits, there is a clear conflict of ethics in the situation of seeking a balance between the federal government, the customers, and the companies providing the products and services. The FBI has repeatedly sought to press for laws that would make it easier to break into devices. As encryption in software became more effective and increased in decentralization across devices, the federal government becomes more determined in having a direct way of breaking into these smart devices. One noticeable example of this increase in determination by the FBI and other law enforcement agencies was demonstrated in March 2019. Facebook CEO Mark Zuckerberg announced that Facebook as a whole would be adopting end-to-end encryption as well as integrate it for their branching services, WhatsApp, Instagram Direct, and Facebook Messenger. This was to be part of a new direction that the company would be adopting, known as a privacy-focused vision for social networking (Watney, 2020). This move would result in more security and privacy for users of Facebook and its branching services, as well as increased encryption of stored data and communications between users. Only the user who sent the message and the user who receives the message would be able to access and read its information. Another form of encryption that Zuckerberg mentioned that would potentially be used is one that locks the device and prevents anyone from accessing it and reading the information except for the owner of the device that owns the key to unlock the device.

This particular move from Facebook and from Zuckerberg himself caught the attention of law enforcement agencies and government officials, and it led to them responding with concern and opposition. Similar to the American government’s response through Former Attorney General William Bar and former Homeland Security Acting Secretary Kevin McAleenan, British and Australian government officials sent letters to Mark Zuckerberg demanding him that he call off his plan of implementing end-to-end encryption in Facebook’s services without making sure that law enforcement agencies are able to access the devices lawfully. On the other hand, civil society organizations sent letters of their own and requested to Zuckerberg that he continue security and encryption measures within Facebook’s services and to not allow for the creation of backdoors (Watney, 2020).

**Allowing Backdoor Access**

**Impacts of Allowing Backdoor Access**

If these companies allow backdoor access to the federal government within encrypted devices and personal company services, it can potentially impact the company’s long-term performance and reception as a business, financially and socially. Public relations are crucial to maintain for a large and influential media company that operates across America and internationally as well. Perception from the customers towards the company that they purchase their products from can greatly affect the companies because of how much their success depends on widespread popularity and satisfaction. The larger the company is in scale and location, then the harder the company will be hit in all areas if a problem such as privacy and security become widespread or vocal as a result of unsatisfied or concerned consumers.

When it was revealed that the FBI would be using wiretappings in backdoors for digital surveillance and push for companies to create backdoors that they could use to access encrypted devices and data, it left a bitter taste of distrust and uncertainty between the technology companies and many of their consumer demographics. Because of that uncertainty and distrust, it made consumers less likely to purchase or download and use the products made by the technology companies, resulting in losses for investments and sales. Facebook’s privacy scandals that took place in the past are an example of these types of hard-hitting incidents.

One of these scandals involved the company gathering personal data that identified large amounts of people was collected with the help of an app called “thisisyourdigitallife.” Through this app, the company was able to create a mass profile of users using this data and the app, in which each user had their digital Facebook information and interactions on the platform exposed. Broad terms and conditions, developer abuse, and lack of any safeguards against data harvesting are factors that allowed this to happen (Watney, 2020).

There has also been certain disconnect in terms of defining what counts as “privacy” between Facebook and the users that advocate for increased privacy measures. Privacy experts and users that advocate for increased privacy measures believe that Facebook should be collecting and retaining less information from its users as a whole, whereas Facebook views increased privacy as limiting the amount of information that is visible to others while that same information is present on the platform. The advokes believe in “less data altogether” while Facebook believes in “less visible, but with the same data as before.” This disconnect and division between the two sides can also contribute to poor public relations and eventually damage in company profits. If positive public relations is to be pursued, then the company must be able to have empathy with their customers as well as find common ground of understanding with them (Watney, 2020).

**Conclusion**

Granting the federal government backdoor access can allowed for the solving of crimes and protection of citizens from dangerous criminal activity, but at the same time, it can also expose people to potential spying by the government. Because of how quickly advancing technology in devices and digital services are taking part in civilian life, it can make things potentially more complicated in cracking down on certain criminal activity in America, as well as raise fears within society that use this increasingly accessible technology in the forms of electronic goods and services. By placing the privacy of customers at stake for the benefit of the federal government, even if the intentions by the company are positive, it will not only potentially cause businesses to suffer in reception and sales as a result of poor public relations, but also in future project development too. At the same time however, law enforcement will be able to crackdown more on crimes more easily within the digital environment that would normally be too difficult or problematic in stopping or being quickly tracked down. While there would be widespread paranoia and losses inflicted upon businesses and media companies such as Google, Twitter, Facebook, and Apple, there would also be better security against criminals that use encrypted smart devices and may potentially leave behind evidence in them that can prove their actions in court cases. Such access granted to the federal government might be able to bring better security benefits among the population, but it is absolutely crucial that the government is monitored to respect the rights of the personal security of citizens nationwide and honoring of personal privacy in a way that is both dignified and justified. With an establishment of reciprocal cooperation between media companies and the federal government, a balance can be achieved in which the companies can help the government in eliminating crime using their technology while at the same time maintain protection of customer information and data (Lear, 2018).

References

Corrigan, J. (2019). DOJ makes another plea for encryption backdoors.*Nextgov.Com (Online),*

Corrigan, J. (2019, Oct 03). Attorney general, DHS secretary call on facebook to build encryption backdoors.*Nextgov.Com (Online),*

FBI wants google facebook to provide wiretap backdoor report 628974. (2012). *EWeek (New York, N.Y.),*

Lear, Shannon. “The fight over encryption: reasons why congress must block the government from compelling technology companies to create backdoors into their devices.” *HeinOnline*, 8 Mar. 2021,

Marks, B. J., & Corrigan, J. (2018). Lawmakers question FBI's push for backdoors in encrypted devices.*Nextgov.Com (Online),*

Watney, M. (2020, July). Law enforcement access to end-to-end encrypted social media communications. In *7th European Conference on Social Media ECSM 2020* (p. 322).

Zhang, J. (2016). Exceptional Access: how a "back door" could create large-scale security threats.*Chicago Policy Review (Online),*