Ultius, Inc.

Writing Samples

23 July, 2016

The Burr-Feinstein Encryption Bill

The tech world is in a tizzy. On April 13, 2016, Senator Richard Burr, Republican from North Carolina, and Diane Feinstein, Democrat from California introduced draft legislation entitled *Compliance with Court Orders Act of 2016* (Maisto). The intent of the bill is to stop circumstances, like those which occurred recently, when *Apple, Inc*. refused to devise software which would unlock an *iPhone's* encryption restrictions for the *Federal Bureau of Investigation* (FBI). Burr and Feinstein are the chair and vice chair of the *Senate Select Committee on Intelligence*, respectively. The objective of the bill is to establish that "everyone must comply with court orders to protect America from criminals and terrorists" (Maisto). Burr and Feinstein stated that the proposed bill is supported by William Bratton, the incumbent *New York City Police Commissioner*, the *National District Attorneys Association*, the *FBI Agents Association*, and other groups. The essence of the bill would require organizations to provide court ordered information when requested, in a format that is readable, and "decrypted, deciphered, decoded, demodulated, or deobfuscated to its original form" (Maisto). The *FBI Agents Association's* president, Reynaldo Tariche, wrote to Burr and Feinstein in support, stating that the legislation would allow Americans and companies to retain hard won privacy protections obtained over hundreds of years. Public and stakeholder input will be solicited prior to formal bill introduction (Feinstein). Burr stated that based on initial reactions, debate on the subject matter has already begun. The chairpersons are optimistic that discussions will go well, and are hopeful about meeting with those who have constructive contributions to make on such an important and

challenging topic. The key to the legislation is that no one is above the law. If a court requires the information, the information should be provided. We live in difficult times today, and in order to foil plots instigated by terrorists and bad actors, law enforcement needs the ability to gain access to information that might aid in preventing the death of Americans. This need is a higher objective than that of protecting privacy (Feinstein).

On the other side of the table, a tech coalition representing numerous technology entities prepared an open letter to Burr and Feinstein (Maisto). In it concern was voiced for what was described as "well-intentioned but ultimately unworkable policies around encryption that would weaken the very defenses we need to protect us from people who want to cause economic and physical harm" (Maisto). Among the coalition's constituency were such organizations as the *Computer & Communications Industry Association*, the *Entertainment Software Association*, the *Internet Infrastructure Coalition* (I2C), and the *Reform Government Surveillance* (RGS). The coalition was concerned that the bill's requirement would cause software design modifications that would negatively impact the expectation of privacy that consumers have come to expect and would create favorable conditions for bad actors to exploit (Maisto). As an unintended consequence of such legislation, bad actors would simply go international in seeking the safeguards they seek, thus diluting the worldwide competitiveness of the United States technological industry, and causing those bad actors to relocate information to off-site global warehouses. The coalition stated that it supports law enforcement's need to protect the public through solving crimes and stopping terrorism. Though they warned, these needs should be balanced by the protections warranted for security and digital information (Maisto).

The *Christian Science Monitor* offered an opinion piece that was not reticent in its denouncement of the bill (Maisto). In fact, Sascha Meinrath and Sean Vitka, Director of *X-Lab*

and the *Palmer Chair in Telecommunication at Penn State University*; and counsel for *Fight for the Future* and a fellow with *X-Lab*, respectively, stated that the Burr-Feinstein legislation was "evidence of a dangerous incompetence in congressional leadership that is undermining America's security" (Maisto). The pair further suggested that Burr and Feinstein be removed from their positions on the Senate Select Committee on Intelligence, or, at least not be allowed to undergo reappointment. Further detailing their positions, the pair wrote, "to put it plainly, this bill would, for example, empower the 11 members of the Augustine Band of Cahuilla Indians to demand that every corporation be able to decrypt all online information of any kind, on any American, and be delivered to that tribe . . . If Burr-Feinstein passes, it guarantees that Americans will have worse encryption than the rest of the world" (Maisto).

The bill focuses on covered entities, such as, “device manufacturers, software manufacturers, electronic communication services, remote communication services, providers of wire or electronic communication services, providers of remote communication services, or any person who provides a product or method to facilitate a communication or to process or store data” (Feinstein). The target of the covered entities component of the bill is aimed directly at companies like *Apple*. The corporation is involved in two cases, one that involves one of two perpetrators who allegedly instigated the San Bernardino, California shooting massacre in December (Plummer). The *FBI* wants access to the information contained on the *iPhone*, and requested that *Apple* build backdoor access into the phone’s operating system, so that the *FBI* can gain access to the phone’s contents. In the second case, out of New York, the *FBI* wants Apple to decipher the cell phone’s pin code, so that they could capture the phone contents belonging to a confessed drug dealer (Plummer).

Apple, in its forty-five page response to the *FBI's* appeal of a lower court ruling denying that *Apple* must comply with the *FBI's* request, the company said that the government must make a showing that the involvement of *Apple* is required (Plummer). The technology corporation believes that the *FBI* has what it takes to decode the needed information on its own and does not require *Apple's* involvement. Tim Cook, *Apple's* Chief Executive, said the corporation views themselves as friends of the *Justice Department*, and recognizes that their intentions are good, but the *FBI* is requesting technology of *Apple* that does not exist now, and is software the company views as too dangerous to create (Nakashima). More specifically, what the *FBI* is asking *Apple* to do is to disable the software component that deletes the data on the *iPhone* after ten failed attempts at providing the correct password. This would enable the *Justice Department* to crack the code through the use of millions of random password combinations so that there is no risk of data loss in the process.

The shooting rampage in San Bernardino occurred at the *Inland Regional Center*, on December 2nd, resulting in the death of fourteen people, and injuries to at least twenty-two individuals (Nakashima). The situation consisted of a heavily planned bombing attempt and mass shooting at a county *Department of Health* training and holiday party event (Botelho and Ellis). Syed Rizwan Farook and Tashfeen Malik, married residents of Redlands, fled the scene immediately after, but were later discovered by police and killed in a shootout. Farook, an employee of the health department, burst into the event with his wife and opened fire on the event goers. The couple also had a makeshift bomb making lab in their apartment. A day later, a very observant *UPS* driver noticed that he had a package addressed to the couple's home, subsequent to the shooting, and returned the package to the *UPS* facility for isolation and inspection (Botelho and Ellis).

Apple: The Courts Should not Make Policy

In an attempt to bolster their position, *Apple* referenced comments made by *FBI* Director James Comey, who stated that the courts were not the proper battleground for addressing problematic policy matters (Plummer). Policy matters are the jurisdiction of the legislators. The courts were not made to address issues that are central to the country's core values, regarding matters close to our hearts and minds, relative to technology and balancing ideals.

The *Justice Department* says that *Apple* has changed its stance and it previous course has been diverted (Plummer). A spokesperson for the *Justice Department* said that *Apple* had helped the Department many times before, in assisting them to access information on its *iPhones*. *Apple* has previously been compliant with court application of the *All Writs Act of 1789* (The Act) (Lewis). *The Act* requires that four conditions be met for court ordered compliance to occur: first is the lack of other viable solutions, if there are no other means available, then the initial condition of the *Act* is met. The second conditioned requirement is that there be an independent foundation for subject-matter jurisdiction. The court order must be properly grounded in the subject-matter for which the court has jurisdiction (Lewis). The third conditioned requirement of the *Act* is that the writ itself must be clearly necessitated by the case in question. The final requirement is that the writ must be consistent with the rules of law.

The *Justice Department* declared that this case represents a major shift in *Apple's* position over time (Plummer). *Apple* had previously stated that it would be just a matter of hours for them to access the data on the phone, since they already have the means of ingress. In response, *Apple* argues that the *Justice Department's* reliance upon the *All Writs Act of 1789* is simply "unprecedented" and that its use of the *Act* borders on the verge of a distension of its legitimate authority (Plummer). In the midst of what *Apple* sees as the government's

overreaching, *Apple* states that they do not have the ability to unlock their phones (Nakashima). The company indicated that the newer technology in use by the *iPhone* used by the terrorist, yet owned by the county *Department of Health*, is too technologically advanced to crack in the manner requested. The corporation stated that they do not have the decryption key, either the phone's user, or a person privy to the password would be the only ones with the ability to unlock the phone. In what amounts to being an advertisement on the amazing security benefits of owning an *iPhone*, the company is in steadfast opposition to the needs of the *Justice Department* (Nakashima).

Matt Olsen, former *National Counterterrorism Center* director, and general counsel for the *National Security Agency*, indicated that the government needs to have the ability to gain access to this data in exigent times (Nakashima). American lives have been lost and the information on the phone could identify all of the players in the massacre. On the other hand, Kevin Bankston, the director of an organization called the New America's Open Technology Institute, stated that the court is ordering *Apple* to create malware to sabotage the strong security features it built into its product. He stated that he was not sure if the company could actually create this software, but this would be the start of a slippery slope of compelling other manufacturers to provide the same service (Nakashima). Bankston continued, that it is not just about a phone, but it is about our collective software and devices – if the precedent becomes the standard, it will not bode well for the trustworthiness of all technological devices.

The central question here is one of security versus privacy and the balance that the court and legislators, like Burr and Feinstein must ultimately determine. Should they err on the side of keeping us safe, or allow us and the bad actors to keep our privacy?

Works Cited

Botelho, Greg and Ellis, Ralph. "San Bernardino Shooting Investigated as 'Act of Terrorism.' *CNN*. Turner Broadcasting System, Inc. 5 December 2015. Web. 10 June 2016. <http://www.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html>.

Feinstein, Diane. "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill." *Diane Feinstein Press Release*. 13 April 2016. Web. 10 June 2016. <http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649>.

Lewis, Danny. "What the All Writs Act of 1789 Has to Do With the iPhone." *Smithsonian Magazine*. Smithsonian Institution. 24 February 2016. Web. 10 June 2016. <http://www.smithsonianmag.com/smart-news/what-all-writs-act-1789-has-do-iphone-180958188/?no-ist>.

Maisto, Michelle. "Burr-Feinstein Encryption Bill Rankles Tech Community." *Information Week*. UBM. 21 April 016. Web. 10 June 2016. <http://www.informationweek.com/government/cybersecurity/burr-feinstein-encryption-bill-rankles-tech-community/d/d-id/1325219>.

Nakashima, Ellen. 'Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks." *The Washington Post*. Nash Holdings LLC. 17 February 2016. Web. 10 June 2016. <https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html>.

Plummer, Quinten. "Apple Refuses To Help FBI Unlock iPhone In New York Drug Case: Who Will Have The Last Laugh?" *Tech Times*. Tech Times, Inc. 17 April 2016. Web. 10 June 2016.

<http://www.techtimes.com/articles/150994/20160417/apple-refuses-to-help-fbi-unlock-iphone-in-new-york-drug-case-who-will-have-the-last-laugh.htm>.

Citation information

You are free to use this sample work for reference and research purposes. However, you **must cite it** and provide attribution to the author. The citation is provided below in MLA format.

Ultius, Inc. “The Burr-Feinstein Encryption Bill.” *Free Writing Samples* | *Ultius*. 23 Jul. 2016. Web.

If you need help with MLA style, please visit the Ultius citation style help section. Thanks for playing fairly.