BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law, Business and the Economy

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

FBI Bypasses Apple to Unlock San Bernadino Shooter's iPhone

By Kevin Jones, J.D. Candidate 2018 | April 9, 2016

The ongoing technology war involving the conflict between privacy and security has taken a new twist as the FBI hacked into San Bernadino terrorist Syed Farook's iPhone. Instead of continuing to pursue a lawsuit to force Apple to reveal its encryption secrets, the FBI used an unknown third party to unlock the phone. Apple and news sources have yet to determine the identity of the third party or how exactly the FBI hacked the iPhone. The FBI also has not revealed if they have discovered any material information through the hack.

Sources from CBS have provided some conjecture as to how the FBI potentially bypassed Apple's encryption. The FBI originally began its search into breaking the iPhone 5c's encryption with assistance from Drivesavers, a California company with experience in recovering information from broken iPhones. The Director of Engineering from Drivesavers revealed that the iPhone 5c permits ten attempts to select a password before a privacy safety feature wipes the drive clean. To circumvent this issue, Drivesavers created a mock iPhone that overrides the safety feature to allow unlimited attempts.

No matter the process by which the FBI ultimately cracked the iPhone, many privacy rights scholars have concerns over the FBI's circumvention of the courts. First, if the FBI has figured out a consistent mechanism to break into iPhones, then they may have access to the private information of hundreds of millions of citizens without any type of search warrant. Second, the FBI communicated to local law enforcement departments that they would provide assistance in hacking individual's iPhones in cases where they could provide evidence. While the FBI believes such practices are necessary to ensure the security of U.S. citizens, these practices completely run afoul of citizen's Fourth Amendment privacy rights. Circumvention of the courts to engage in security concerns removes any independent government branch from reviewing the legitimacy of asserted policing concerns.

University of Wisconsin Professor Dietram Scheufele, an expert in media, has specifically addressed a major issue in the public's response to privacy concerns if citizens truly want the FBI to be held accountable. He points out how the temporary public outcry quickly dies down, allowing the FBI to continue their new practices as the "status quo." Scheufele claims, "Consumers are not going to care" because they want a customized experience with apps on the smartphones that require a great deal of private information. However, Scheufele does not worry about the FBI gaining access to individuals' private information. He discusses how Europeans hold an antithetical relationship with data privacy—the government is trusted to be the information holder as opposed to private corporations.

While this case does not provide a definitive answer as to which institutions should serve as the ultimate protector of data privacy, the FBI's ability to circumvent the courts highlights the legal system's inability to keep up with the rapid pace of technology.