By: Erik Buschardt, Summer 2016 Term - Paper #2

Introduction: The Legalities of Cryptography

The legalities of encryption are complex, as they should be with the operation of any powerful tool. This paper will discuss several facets with regards to government regulation of encryption, as well as case studies, and a recent debate held at New York University.

The Right to Privacy v. Legal Pursuits

At issue is a fundamental quest for justice, where the mathematics of encryption acts as an obstacle for law enforcement activity, especially when it comes to evidence thought to have been captured on an encrypted device which may help in either the prosecution or defense of a legal case.

On one hand is the right to privacy as guaranteed by the Fourth Amendment's search and seizure premise. As debated in a previous legal class (CSSS 5210 from Spring I 2016), what is *not* clear is the right to snoop. At what point in a private backyard are all household activities such as barbecuing, guaranteed not to be photographed from a zoom-lens camera mounted to a passing drone, flown from a public domain area above the street?

Let us presume further that said drone belongs to law enforcement with intent to gather evidence (rather than simply paparazzi with intent to sell a magazine), and that the law enforcement has no prior evidence from which to prosecute a case… yet.

From a cryptographic sense, the right to privacy essentially amounts to the right to keep any data, good or bad, encrypted and free from Big Brother. A recent debate highlighted below will emphasize the point of the "For The Motion" prosecution. Phil Zimmerman inflamed this debate via his actions to promote the use of Pretty Good Privacy (PGP). Finally, we are treated to a discussion with regards to the National Security Administration (NSA), Ron Rivest, Adi Shamir, and Leonard Adleman (RSA), and the Computer Act of 1987, whereby the NSA was tasked to provide a definition for such encryptions deemed to be safe enough to break…. But I digress. In reality, the Act authorized the NSA to work with public and private industry in order to develop cryptographic standards. [Singh, S.]

United States v. Fricosu

United States of America v. Ramona Camelia Fricosu, a.k.a. Ramona Smith ("The United States v. Fricosu", No. 10-cr-00509-REB-02, 2012), was a federal criminal case held in the District of Colorado whereby the Fifth Amendment was used in a defense of self-incrimination. Ultimately the ex-husband of the defendant offered a list of passwords, one of which eventually worked to unlock the device in question.

What is interesting about this case is that the All Writs Act of 1789 (28 U.S.C. § 1651) was used in the prosecution, where it was also used in 2016 with Apple's dispute against the Federal Bureau of Investigation (FBI) with regards to possession of the communication device in conjunction with a recent terrorist activity. [The Weak Protection...]

Deniable, Undeniable and Plausible Deniability with respect to encryption policy

For this section I will simply resort to established dictionary definitions, then describe similarities and contrasts. Merriam-Webster defines "deniable" as that which is possible to deny. For example, in U.S. v. Fricosu, the defendant claimed to lose the password under the assumption of the Fifth Amendment's protections offered.

Undeniable is that which is not possible to deny (that which is clearly and proven true). In encryption policy, this would include measures of timestamping and authorization of access for messages and transmissions, which would provide a measure of irrefutability and undeniable evidence. [Deniable], [Undeniable]

Finally, "plausible deniability" is that which senior officials or other such persons can maintain an innocence of malicious actions by claiming to not know the detailed actions of subordinates under their command. Plausible deniability can also be considered that which is the "benefit of the doubt" in a prosecution. Coined in 1960 by the CIA, plausible deniability can exist for any number of covert and overt operations that would not be held to a standard of malicious intent and scrutiny, if such operations were to be exposed to the public.

An example of plausible deniability is cited with respect to Iraq's WMD program, where the term "dual-use facility" was used to obtain plausible deniability for industrial plants. Within the scope of plausible deniability in encryption policy however, a great example would be the

steganographic embedding of data within digital imagery, in order to deny the existence of coded messages, while citing only the existence of the image. [Iraq's Chemical Warfare Program]

Why the NSA is in the middle of this topic?

I would argue that The National Security Administration is in the middle of this topic because not only for the actions of one certain former contractor (Edward Snowden) and his actions performed in 2013 to The Guardian newspaper, but that the hackers at the NSA are best able to hack into any device they want, even more capably than the FBI, who made the mistake of "politely" asking Apple to decrypt their own popular and commercially available series of products, thereby inflaming the public policy debate further. After the successful decryption by the foreign third party, one is led to believe that the legal drama involving the All Writs Act of 1789 was simply a cover story, hiding the deeper policy truths.

FBI as gatekeeper?

First off, it was fantastic to watch a video of a recent policy debate held on April 26, 2016 at New York University where Edward Snowden won the popular vote in a landslide fashion, approx 70% to 22% (9% undecided) against Fareed Zakaria of CNN, (video available at http://www.debatesofthecentury.org/national-security/). What a mockery! Not only did Mr. Zakaria discredit himself several times as "not a technologist", the only technologist he did cite left his own tech firm (Microsoft) in favor of full time philanthropic work in third world countries since 2008.

A highlight of said circus was at the 1:05:15 mark where Mr. Zakaria claimed to have been lucky of not being hacked, by not encrypting his phone, and also where it was joked that Mr. Snowden was "reading [Mr. Zakaria's email] right now (1:06:00). Presidential Colgate toothpaste (1:11:00), the moderator's made up word "fenestra" to represent a governmental mandate of decryption (33:43) a.k.a. Bob's decryption key [Key(b)], [Fenestra], Chernobyl (1:15:20), and even kittens as a devil's advocate (Snowden: "if I was for kittens, [the NSA would] be completely against them") were also thrown into the debate just for fun as well.

Finally per the debate, it was noted that encryption was about the empirical science, specifically mathematics and advanced number theory, and that as a given definition, this science cannot be placed under doubt nor compromise. Per Mr. Snowden, the mathematics remain certain and absolute. Either we will continue to employ the mathematics in order to protect our devices from interception from Eve, Oscar, Big Brother or any foreign government, or we do not have any useful or effective encryption methodologies at all. Therefore, there can be no compromise of the application of the powerful mathematics used.

Thus in light of this video debate and also due to prior beliefs and convictions regarding this topic stemming from my engineering and mathematics courses from undergraduate studies, I firmly do not believe the FBI should require companies to maintain access to communication devices or services of any kind. Such a limitation on technical innovations would paralyze any further efforts to provide consumer protections, and would critically expose all commercial and personal transactions unnecessarily.

I believe further that since the Israeli decryption of the San Bernardino iPhone, the FBI has been chasing *policy* and legal precedent in order to pursue further enforcement activity, and that it was never a technical debate against Apple per se.

Conclusions and Final Thoughts

Like I mentioned previously, legal entanglements involved with the enforcement of any powerful set of tools such as modern digital encryption can and should be treated with the same checks and balances that were designed into any Westminister-ian (or Jeffersonian, if you prefer) democratic system, and indeed do seem to be headed down the judicial paths of prosecution and defense when conflicts regarding the encryption process occur.

While I don't see this pattern of policy conflict ending anytime soon, we have gained an understanding of its underlying science, the growth of the field as even more sophisticated algorithms come into more common use with more advanced hardware, and we will be therefore better positioned to better our national defenses against known threats, just as in any traditionally kinetic wartime or peacetime mission.

References

Deniable. 2016. In Merriam-Webster.com.
Retrieved July 20, 2016, from http://www.merriam-webster.com/dictionary/deniable

Fenestra. 2016. In Merriam-Webster.com.
Retrieved July 20, 2016, from http://www.merriam-webster.com/dictionary/fenestra

Iraq's Chemical Warfare Program. (2007, January 23). Retrieved July 20, 2016, from
https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/chap5.html

Singh, S. (2000). *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography*. Anchor Books.

The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege, VANDERBILT J. OF ENT. AND TECH. LAW [Vol. 12:3:581] Retrieved July 20, 2016
from http://www.jetlaw.org/wp-content/journal-pdfs/McGregor_online.pdf

Undeniable. 2016. In Merriam-Webster.com.
Retrieved July 20, 2016, from http://www.merriam-webster.com/dictionary/undeniable

Wagner Search. (2016, April 29). Retrieved July 20, 2016, from
http://wagner.nyu.edu/news/newsStory/
debates-century-features-snowden-and-zakaria-national-security