The Battle for Backdoors and Encryption Keys

Article · July 2021

DOI: 10.14302/issn.2766-8681.jcsr-21-3789

1 author:

Donald L. Buresh
Morgan State University
82 PUBLICATIONS **59** CITATIONS

OPEN ACCESS
Freely Available Online

JOURNAL OF CURRENT SCIENTIFIC RESEARCH

ISSN NO: 2766-8681

Review

DOI: 10.14302/issn.2766-8681.jcsr-21-3789

The Battle for Backdoors and Encryption Keys

Donald L. Buresh, Ph.D., J.D., LL.M.[1,*]

[1]Morgan State University Cybersecurity and Policy Department.

Abstract

This paper argues that the use of backdoors in software is inherently counterproductive and leads to invasion of privacy, either by federal or state governments or by intrusive hackers. The essay outlines encryption's nature, pointing out that a software backdoor is a secret means of ignoring data authentication. Several examples of known backdoors known to terrorists, criminals, and governments alike are highlighted. Arguments in favor and opposing backdoors are provided, where the Apple Computer, Inc. v. FBI controversy is discussed. Finally, the balancing of harms test as proposed by John Stuart Mill is introduced, where the article concludes that when balancing the opposing positions, the scale tips toward data encryption because an innocent party would suffer the most harm from the existence of a software backdoor.

Corresponding author: Donald L. Buresh, Ph.D., J.D., LL.M. Morgan State University, Cybersecurity and Policy Department.

Keywords: Apple Computer, Inc. v. FBI, Backdoors, Balancing of Harms, Ciphers, Encryption Keys

Recieved: Mar 30, 2021 **Accepted:** Jul 06, 2021 **Published:** Jul 09, 2021

Editor: Shailendra Dwivedi, University of Oklahoma, Department of Obstetrics and Gynecology.

Introduction to Encryption

In cryptography, encryption is a mechanism whereby a message or information is encoded to access the data, and unauthorized parties cannot obtain the data.[1] Encryption does not prevent an individual from accessing data, but it does stop persons from getting the data's content.[2] With encryption, data is encrypted using a cipher.[3] Typically, an encryption scheme employs a pseudo-random encryption key that is created by a pre-specified algorithm.[4] Although it is logically possible to decrypt data without a key, it requires considerable technical skill that is usually beyond most people's grasp.[5]

Encryption keys can either be symmetric or asymmetric.[6] When an encryption key is symmetric, the same key is used to encrypt and decrypt data.[7] When an encryption key is asymmetric, one key is used to encode information, and another key is employed to decode data.[8] The key used to encrypt data is a *public key*. It is available for everyone to use, whereas the key applied to decrypt information is called a *private key*, and only specific individuals possess this key.[9] Diffie and Hellman first developed asymmetric keys in 1976.[10] A popular asymmetric encryption methodology is *Pretty Good Privacy* ("PGP") which Phil Zimmermann created in 1991.[11] In 2010, the method was purchased by Symantec Corp. which updates PGP periodically.[12]

Encryption has existed for thousands of years. Julius Caesar employed a rotating cylinder to form a simple substitution cipher.[13] George Washington suggested using so-called "invisible ink" when communicating with his staff.[14] During World War II, the Germans created an enigma machine that produced a polyalphabetic substitution cipher that changed daily.[15] In 2007, the Computer Security Institute reported that 71 percent of firms employed encryption for some of their data transmissions, while 53 percent of companies surveyed encrypted their data held in storage.[16]

Cyber-criminals have developed sophisticated attacks in response to encryption, encompassing cryptographic attacks, stolen ciphertext attacks, encryption key attacks, corporate insider attacks, data corruption attacks, data destruction attacks, and ransomware attacks.[17] Defenses include data fragmentation and active defense data protection technologies such as moving or mutating ciphertext, thereby ensuring that it is somewhat challenging to identify, steal, corrupt, or destroy.[18]

One of the essential features of encryption is that it can be used to protect data in transit. Examples include data being transferred over the Internet, mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices, and even bank automatic teller machines.[19] Data in transit can be intercepted, but it is pretty challenging to determine the data's content when it is encrypted.[20]

Even though data are encrypted, additional techniques are needed to verify whether a message is authentic.[21] For example, digital signatures are used to ensure a message's authenticity through a message authentication code ("MAC").[22] The issue is that a single system design error can be exploited in a successful attack.[23] Furthermore, it sometimes happens that unencrypted information can be obtained without decrypting the data.[24] The process employs software known as a Trojan after how Odysseus and the Greeks defeated the City of Troy in Homer's epic poem, *The Illiad*.[25] Data tampering can be avoided by employing digital signatures along with encryption.[26]

What is a Backdoor?

A backdoor is precisely what the word means. It is a secret method of ignoring data authentication or encryption so that the content of information can be accessed clandestinely.[27] A backdoor can be part of a computer program; it can be a separate program or specific hardware.[28] One legitimate type of backdoor is where a manufacturer includes a mechanism in its software or device that allows the company to restore user passwords.[29] A default password can also serve as a backdoor provided that a user does not alter the password.[30]

Petersen and Turn first addressed computer subversion in a 1967 American Federation of Information Processing Societies ("AFIPS") Conference paper.[31] The authors talked about a collection of active infiltration attacks that employed "trap door" entry points into a computer system, sidestepping security

and allowing seemingly carte blanche to assess data.[32] Because of the beginning of public encryption keys, the term "trap door" yielded to the term "backdoor," particularly in J.P. Anderson and D.J. Edwards's work in 1979.[33]

In a computer system where a user logs into a computer, a backdoor could be construed as a hard-coded username and password.[34] One application where this kind of backdoor has existed for years is telephone communication software.[35] A traditional backdoor is symmetric, where anyone that discovers the backdoor can use it. In contrast, an asymmetric backdoor was pioneered by Young and Yung and can only be accessed by an individual who embeds the backdoor in a computer system.[36] It is computationally intractable to find an asymmetric backdoor using a black-box query.[37] This type of attack is known as *kleptography*, and it can be implemented in hardware and software.[38] A different kind of backdoor uses a compiler and a set of object-code library routines containing the back door.[39] The backdoor becomes part of a program when it is compiled using the object-code library to form an executable program and was alluded to Thompson when he gave his Turing Award speech in 1984.[40]

When a backdoor is open, it is somewhat difficult to close. One way to counter an attack using a backdoor is to rebuild the system from scratch, creating the executable code by employing a different compiler.[41] In practice, this procedure is rarely done by end users due to their lack of computing sophistication.[42] Better to create a clean system no matter how annoying this process may seem to be.[43]

Examples of Backdoors

There are a variety of known backdoors. The United States federal government has proposed that vendors create hardware backdoors so that law enforcement can access the computers and cell phones of known terrorists and other criminals.[44] These backdoors include:

The Clipper Chip – This was a device designed by the National Security Agency ("NSA") that employed a specialized chip known as *Skipjack* that would give law enforcement access to all encrypted data communications. The chip was introduced in 1993. It was promoted by the government as a voluntary plan but was not well received due to ideological reasons;[45]

The Clipper Chip II

This was a modification of the Clipper Chip, where it was suggested that the chip employ a 56-bit DES encryption methodology. However, in 1996, the chip failed to win business support because it was felt that 56-bit DES encryption was too weak to stop would -be hackers from successfully attacking devices that contained the chip;[46] and

Key Management Infrastructure or Clipper III

This methodology focused on key management infrastructure which was based on the presumption that all public keys would possess a duly authorized certificate. This backdoor met with the same criticism that was levied at Clipper Chip II. Primarily, the proposed 56-bit DES encryption was too weak to ensure the security of an encryption key.[47]

Historical Backdoors

1. *Back Orifice* – This backdoor was created in 1998 by the Cult of the Dead Cow. It permitted Windows computers to be remotely controlled over a network;[48]
2. *The Dual_EC_DRBG* is a cryptographically secure pseudo-random number generator with a kleptographic private key backdoor that was deliberately put into the NSA's software. This fact was publically announced in 2013;[49]
3. *Several unlicensed copies of WordPress plug-ins* were found in March 2014 to possess several backdoors in JavaScript code;[50]
4. *Borland Interbase versions 4.0 through 6.0* maintained a hard-coded backdoor that Borland software developers created. The server source code contained a compiled-in backdoor account (i.e., username: "politically" and password: "correct") that was accessible over a network connection;[51] and
5. *Juniper Networks* contained a backdoor inserted in 2008 to the *ScreenOS* firmware from versions 6.2.0r15 to 6.2.0r18 and from versions 6.3.0r12 to 6.3.0r20. The backdoor provided a user with

administrative privilege.[52]

Arguments Favoring and Opposing Backdoors

The first subsection discusses the government's arguments for installing backdoors, whereas the second subsection talks about why the industry opposes backdoors. The government's statements are based on public safety issues. The industry urges that backdoors are either logically impossible or nullify existing security measures.

Arguments Favoring Backdoors

The arguments by the government in favor of technology companies implementing hardware or software backdoors are practical rather than ideological.[53] The government argues that the federal government needs backdoors into these machines because it will make America safer by allowing law enforcement to easily capture and prosecute terrorists and other cybercriminals.[54] The government claims will not enhance the ability to thwart the encryption algorithm. There would be a minimal impact on cybersecurity.[55]

The argument has some merit when the various nation-states are asymmetrically employing cyber-attacks.[56] In other words, militarily weaker states are using cyber espionage techniques to gather the information that could be used to help even the economic or military playing field.[57] In particular, NSA director Michael Rogers observed that: "[i]f you look at the topology of [the] attack from North Korea against Sony Pictures Entertainment, it literally bounced all over the world before it got to California."[58] The implication was that if there were technological backdoors both in hardware and software, Sony Pictures together with the government would have substantially mitigated the effect of the attack.[59] According to Rogers, the United States government is playing catch-up regarding cybersecurity.[60]

Furthermore, Christopher Wray, the current director of the Federal Bureau of Investigation ("FBI"), pointed out that at the International Conference on Cyber Security that was held in New York City in 2018 that in 2017, the FBI seized 7,775 devices that it was unable to unlock because of encryption.[61] Wray claimed that this was a significant public safety issue because the cases dealt with human trafficking, counterterrorism, organized crime, and child exploitation.[62] What Wray desired is encryption that is secure from the outside world but is available only for law enforcement to exploit.[63]

Arguments Opposing Backdoors

According to Pfefferkorn, a severe problem with the government's request is that the desired government's technical requirements are either unclear or unknown.[64] In both public speeches and interviews, both then Deputy Attorney General Rodney Rosenstein and the FBI

Director Christopher Wray has requested technological changes in electronic devices that would facilitate improved law enforcement. Rosenstein has suggested that: "manufacturers could manage the exceptional-access decryption key the same way they manage the key used to sign software updates.[65]" Wray has indicated that electronic devices should provide data security along with lawful access.[66] The problem with both of these proposals is that they are pretty vague. Both Rosenstein and Wray were echoing their desire to gain access to electronic devices without the necessity of first obtaining a warrant. Both individuals were recommending that the key to the backdoor be held in safekeeping until law enforcement wanted to access the content of a device.[67]

Pferrerkorn offered the following four arguments why Rosenstein's and Wray's requests do not make good sense.[68] First, there are too many law enforcement agencies that would request the backdoor encryption keys for mobile devices.[69] Demands for backdoor encryption keys could be made several times in a day.[70] In other words, the backdoor encryption would no longer be secure because too many law enforcement people would know what it was.[71] The risk of loss could well be catastrophic.[72] Second, cyber attackers would probably be able to obtain the key by spear-phishing and whaling.[73] Third, the market share of cell phone sales, both in the United States and throughout the world, would decline because security could not be guaranteed.[74] Finally, Pfefferkorn aptly pointed out that if the content of a communication is encrypted, law enforcement would have to break the

content-encryption code to understand the content of the information on a computer or a mobile device.[75]

Then there is the issue of metadata. In *Carpenter*, the Court opined that the government violated Carpenter's Fourth Amendment rights in obtaining cell phone metadata without a warrant.[76] Before *Carpenter*, the government could get cellphone metadata by merely asking for it from the cell phone provider, stating that the data was needed for an investigation. The ruling in *Carpenter* was relatively narrow because it did not opine on whether the cellphone user or the cellphone provider owned the metadata.[77] Strangely, the cellphone user's property rights were not discussed in the majority opinion even though property rights formed the basis of the Sixth Circuit judgment.[78] The good news from *Carpenter* is contained Justice Gorsuch's dissent, where he stated that cell phone metadata is the property of cell phone owners.[79] His objection is insightful because if cell phone owners have a reasonable expectation of privacy, it is a small step to allowing individuals to control the data about themselves that others can see on the Internet. Currently, based on the sheer volume of metadata, law enforcement can quickly obtain and then infer the content of the data based solely on location metadata.[80]

Issues with Backdoors and Encryption

First, the government does not need backdoor technology because it already has the technology to break into computers and mobile devices. Second, when conducting a balancing of the harms test[81] and applying Mill's principles contained in *On Liberty*,[82] it is apparent that backdoors do more harm than good.

Counter Example to the Government's Argument

The government's arguments in favor of backdoors are seemingly unpersuasive. Consider the *Apple Computer v. FBI* controversy of 2015-16. On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik killed 14 people and injured 22 others while attacking a San Bernardino County Department of Public Health Christmas party and training event.[83] Four hours later, they were both killed by the police in a shootout.[84]

On February 9, 2016, the FBI revealed that it could not unlock Farook's iPhone 5C cell phone.[85] The FBI asked the National Security Agency ("NSA") to hack the phone, but the NSA could not do it.[86] The FBI then asked Apple to create a new version of the cell phone's iOS operating system installed on the phone, disabling its security features. Apple refused because of its pro-security policies. The FBI then asked a federal court to require Apple to implement the operating system's change under the All Writs Assistance Act of 1789, not a warrant nor a subpoena. Apple opposed the order, stating that no government agency had ever issued such a subpoena.[87]Apple was given until February 26, 2016, to comply with the court order.88

On February 19, 2016, the Department of Justice ("DOJ") filed a new motion in federal court to compel Apple to comply with the February 9, 2016 court order.[89] Because Farook was a San Bernardino County employee, the FBI asked the County to reset Farook's iCloud password so that the data could be obtained directly from the cloud; however, this procedure prevented the cell phone from copying recent data to the cloud.[90]

On March 28, 2016, the DOJ made it known that it had unlocked Farook's iPhone, and the suit against Apple was withdrawn.[91] In September 2016, the Associated Press, Vice Media, and Gannet Publishing filed a Freedom of Information Act ("FOIA") lawsuit against the FBI, demanding that the government agency divulge the organization's name that had hacked Farook's iPhone.[92] On September 30, 2017, a federal court granted the FBI's motion for summary judgment, citing that the name of the company and the amount of money to the firm were national security secrets, thereby making the issue moot and no longer ripe for adjudication.[93]

Based on this example, it is evident that the FBI does not need a backdoor to open up a cell phone.

The Balancing of the Harms

According to John Stuart Mill in his essay *on Liberty*, an individual has the freedom to think and to emote, including the freedom of speech.[94] A person also has the freedom to follow one's tastes (including immoral tastes) provided that no harm comes to

others.[95] Thirdly, people have the freedom to unite with others, provided that the individuals are adults, there is no compulsion, and no harm comes to others.[96] These three principles promote encryption in communication because a person to think, emote, and speak without fear of governmental interference. Suppose electronic devices have backdoors where the government can intercept messages. In that case, there is the distinct possibility that people will be afraid to speak their minds to other for fear of governmental retribution.

Mill's objections to government intrusion promote encryption by private companies.[97] The reason is that with encryption private firms will protect their customers' data because the consequence of not protecting the data is an almost immediate loss of business and profits.[98] Even if the government is better qualified to defend its citizens, Mill would argue that private organizations should protect customer data because, in the long-run, the profit motive will yield better results than government outcomes.[99] Furthermore, the fact that a backdoor encryption key has the potential to encourage an over-reaching and over-powering government, Mill would argue that backdoors should be avoided.[100]

Consider the *balancing of the harms test*.[101] As the custodian of public safety, the government argues that it has a responsibility to protect American citizens.[102] The harm to the average American is nebulous because very few individuals are exposed to terrorist attacks.[103] In contrast, the existence of a backdoor in a computer operating system or a cell phone almost assures cybercriminals will breach that personal information.[104] Thus, employing the balancing of the harms test, the harm to individuals is far more significant than the vague threats to public safety.

Finally, encryption and private keys are much more often than not concerned with private communications among citizens that have nothing to do with law enforcement.[105] Also, according to Mill, most actions by individuals do not prejudice the interest of others.[106] This means that for the innocent people who would be subjected to government intrusion into their privacy, a backdoor encryption key is a detriment, mainly if cyber-attackers were to discover the key and then use that knowledge for nefarious ends.[107] If one considers Mill's philosophy on liberty and government interference, it becomes readily apparent that Mill would be against backdoor encryption keys. In short, when employing a *balancing of the harms test*,[108] in my opinion, Mill would be against backdoor encryption keys because an innocent individual is a party that would suffer the most harm from the existence of a backdoor.

Conclusion

Therefore, on practical grounds, the government does not need backdoor encryption keys. The *Apple Computer v. FBI* example demonstrates this conclusion. On ideological and philosophical foundations, as espoused by Mill, there is no good reason for private industry to appease the government by giving it a backdoor encryption key that cyber-attackers would readily discover in short order.

So why does the Justice Department insist that electronics manufacturers insert a backdoor into their products? The answer could be as simple as dollars and cents. The government does not want to pay a consultant or an employee to unlock a mobile device virtually on demand. It seems that the government wants instant access to a mobile device without expending any effort. There could be a nefarious reason that only a conspiracy theorist would imagine. It could be any one of the above reasons or even some other reason. Who knows? But one thing is for sure, the federal government knows.

Reference

1. *Cryptography*, Merriam-Webster's Dictionary, n.d., https://www.merriam-webster.com/dictionary/cryptography.
2. Greg Schulz, *Top 10 ways to secure your stored data*, ComputerWorld, August 3, 2006, https://www.computerworld.com/article/2546352/data-center/top-10-ways-to-secure-your-stored-data.html.
3. *Cipher*, Merriam-Webster's Dictionary, n.d., https://www.merriam-webster.com/dictionary/cipher.

4. Ben Lynn, *Pseudo-Random Number Generators*, Stanford University, n.d., https://crypto.stanford.edu/pbc/notes/crypto/prng.html.
5. Brooks Cunningham, *No Private Key, No Problem. How to Decrypt SSL Traffic with Session Keys*, Citrix, (February 20, 2015), https://www.citrix.com/blogs/2015/02/20/no-private-key-no-problem-how-to-decrypt-ssl-traffic-with-session-keys/.
6. *Description of Symmetric and Asymmetric Encryption*, Microsoft Support, n.d., https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption.
7. Id.
8. Id.
9. Id.
10. Whitfield Diffie & Martin Hellman, *New Directions in Cryptography*, 22 IEEE Transactions on Information Theory 6, (November 1976), 644-54, https://ee.stanford.edu/~hellman/publications/24.pdf.
11. *History*, OpenPGP, (August 15, 2016), https://www.openpgp.org/about/history/.
12. Jeremy Kirk, *Symantec buys encryption specialist PGP for $300M*, ComputerWorld, (April 29, 2010), https://www.computerworld.com/article/2517739/security0/symantec-buys-encryption-specialist-pgp-for--300m.html.
13. Dennis Luciano & Gordon Prichett, *Cryptology: From Caesar Ciphers to Public-Key Cryptosystems*, 18 The College Mathematics Journal 1, 2-17, (January 1987), http://www.math.stonybrook.edu/~moira/mat331-spr10/papers/1987%20LucianoCryptology%20From%20Caesar%20Ciphers%20to.pdf.
14. *Spy Techniques of the Revolutionary War*, George Washington's Mount Vernon, (n.d.), https://www.mountvernon.org/george-washington/the-revolutionary-war/spying-and-espionage/spy-techniques-of-the-revolutionary-war/.
15. Alan Stripp, *How the Enigma Works*, Nova: Public Broadcasting System, (November 11, 1999), http://www.pbs.org/wgbh/nova/military/how-enigma-works.html.
16. Robert Richardson, *2008 CSI Computer Crime & Security Survey*, Computer Services, Inc., (2008), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.
17. Gérard Memmi, Katarzyna Kapusta, Patrick Lambein, & Han Qiu, *Data Protection: Combining Fragmentation, Encryption, and Dispersion, Final Report*, (November 2016), https://arxiv.org/ftp/arxiv/papers/1512/1512.02951.pdf.
18. Id.
19. John Padgette, Karen Scarfone, & Lily Chen, *Guide to Bluetooth Security: Special Publication 800-121 Revision 1*, National Institute of Standards and Technology, (June 2012), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-121r1.pdf.
20. Sandra Kay Miller, *Fiber optic networks vulnerable to attack*, TechTarget, (November 15, 2006), https://searchsecurity.techtarget.com/news/1230106/Fiber-optic-networks-vulnerable-to-attack.
21. *Message Authentication Code – MAC*, Investopedia, (n.d.), https://www.investopedia.com/terms/m/message-authentication-code.asp.
22. Dawn M. Turner, *What is a Digital Signature - What it Does, How it Works*, CryptoMathic, (December 10, 2015), https://www.cryptomathic.com/news-events/blog/what-is-a-digital-signature-what-it-does-how-it-works.
23. Jerome Carter, *Diagnostic Error, Results Management, and Software Design*, EHR Science, (February 20, 2016), https://www.ehrscience.com/2016/02/29/diagnostic-error-results-management-and-software-design/.
24. Brooks Cunningham, *supra*, note 5.
25. *What is a Trojan Virus? – Definition*, Kaspersky Lab, (n.d.), https://usa.kaspersky.com/resource-center/threats/trojans and HOMER & ROBERT

FAGLES, THE ILLIAD (Penguin Classics Reissue edition 1998).

26. Dawn M. Turner, *supra*, note 22.
27. Kim Zetter, *Hacker Lexicon: What Is a Backdoor?*, Wired, (December 11, 2014), https://www.wired.com/2014/12/hacker-lexicon-backdoor/.
28. Id.
29. Rajendra Choudhary, *How to Reset Windows Password through a Backdoor*, Moonking Hackers Club, (January 24, 2016), http://moonkinghackersclub.com/how-to-reset-windows-password-through-a-backdoor/.
30. Id.
31. H. E. Petersen & Rein Turn, *System Implications of Information Privacy*, Rand Corporation, (April 1967), https://www.rand.org/pubs/papers/P3504.html.
32. Id.
33. Willis H. Ware (ed.), *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1*, Rand Corporation, (October 1979), https://www.rand.org/pubs/reports/R609-1/index2.html.
34. Kim Zetter, *supra*, note 27 and Rajendra Choudhary, *supra*, note 29.
35. About 20 years ago, the author worked for a company tha developed telecommunications software that was sold to the major telecommunications companies. The software that was quality assured possessed a backdoor whereby an authorized individual within one of the telecommunications company could log in using the backdoor and examine the landline telephone conversations of the company's customers. This was the first time that the author became aware that backdoors for software applications existed.
36. Young & Yung, *Cryptovirology: extortion-based security threats and countermeasures*, Proceedings 1996 IEEE Symposium on Security and Privacy, (May 6-8, 1996), https://ieeexplore.ieee.org/document/502676/?reload=true.
37. Andrew Ilyes, *Black-box Adversarial Attacks with Limited Queries and Information*, Labstx, (April 22,2018), https://www.labsix.org/limited-information-adversarial-examples/.
38. *Kleptography*, Collins English Dictionary, (n.d.), https://www.collinsdictionary.com/us/submission/15694/Kleptography.
39. Ken Thompson, *Reflections on Trusting Trust*, Communications of the ACM: Turing Award Lecture, (August 1984), https://www.archive.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf.
40. Id.
41. David A. Wheeler, *David A. Wheeler's Page on Fully Countering Trusting Trust through Diverse Double-Compiling (DDC) - Countering Trojan Horse attacks on Compilers*, George Mason University: Author's 2009 Ph.D. Dissertation, (2009), https://www.dwheeler.com/trusting-trust/.
42. Id.
43. Id.
44. Iain Thompson, *FBI says it can't unlock 8,000 encrypted devices, demands backdoors for America's 'public safety'*, The Register, (January 9, 2018), https://www.theregister.co.uk/2018/01/09/fbi_boss_backdooring_encryption/.
45. RICHARD A. SPINELLO, CYBERETHICS: MORALITY AND LAW IN CYBERSPACE 214-16 (Jones Bartlett Learning 5th ed. 2014).
46. Id.at 216.
47. Id. at 216-18.
48. Matt Richtel, *Hacker Group Says Program Can Exploit Microsoft Security Hole*, The New York Times: Cybertimes, (August 4, 1998), https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/cyber/articles/04hacker.html.
49. Kim Zetter, *How a Crypto 'Backdoor' Pitted The Tech World against the NSA*, Wired, (September 24, 2013), https://www.wired.com/2013/09/nsa-backdoor/.
50. Denis Sinegubko, *Joomla Plugin Constructor Backdoor*, Securi.net, (April 23, 2014), https://

blog.sucuri.net/2014/04/joomla-plugin-constructor-backdoor.html.

51. M. Edwards, *Borland Interbase Server Contains Backdoor Account*, ITPro Today, (January 9, 2001), https://www.itprotoday.com/security/borland-interbase-server-contains-backdoor-account.
52. Sean Gallagher, *Researchers confirm backdoor password in Juniper firewall code*, ARS Technica, (December 21, 2015), https://arstechnica.com/information-technology/2015/12/researchers-confirm-backdoor-password-in-juniper-firewall-code/.
53. Linda Wertheimer (Host), *The Cybersecurity Argument For And Against Device Encryption*, National Public Radio, (December 26, 2015), https://www.npr.org/2015/12/26/461095800/the-cybersecurity-argument-for-and-against-device-encryption.
54. Eyragon Eidam, *Privacy vs. Security: Experts Debate Merits of Each in Tech-Rich World*, Government Technology, (June 7, 2017), http://www.govtech.com/policy/Privacy-vs-Security-Experts-Debate-Merits-of-Each-in-Tech-Rich-World.html.
55. Id.
56. COL. QIAO LIANG & COL. WANG XIANGSUI, UNRESTRICTED WARFARE (Echo Point Books & Media 1999)
57. Id.
58. Tom McCarthy, *NSA director defends plan to maintain 'backdoors' into technology companies*, The Guardian, (February 23, 2015), https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies.
59. Id.
60. Id.
61. Iain Thompson, *supra*.
62. Id.
63. Id.
64. Riana Pfefferkorn, *The Risks of "Responsible Encryption"* 3, The Center for Internet and Society, (February 2018), https://cyberlaw.stanford.edu/files/publication/files/2018-02-05%20Technical%20Response%20to%20Rosenstein-Wray%20FINAL.pdf.
65. Id. at 7.
66. Id. at 4.
67. Id.
68. Kevin Townsend, *The Argument Against a Mobile Device Backdoor for Government*, Security Week, (February 7, 2018), https://www.securityweek.com/argument-against-mobile-device-backdoor-government.
69. Id.
70. Id.
71. Id.
72. Id.
73. Id.
74. Id.
75. Id.
76. See *Carpenter v. United States*, 585 U.S. ____ (2018)
77. Id.
78. See *United States v. Carpenter*, 819 F.3d 880 (6th Cir, 2016).
79. See *United States v. Carpenter*, 585 U.S. ___, Gorsuch's Dissent.
80. Id.
81. *Legal Theory Lexicon: Balancing Tests*, Legal Theory Blog, (August 4, 2013), http://lsolum.typepad.com/legaltheory/2013/08/legal-theory-lexicon-balancing-tests.html.
82. JOHN STUART MILL, ON LIBERTY (John W. Parker & Son 1859).
83. Amanda Lee Myers & Justin Pritchard, *14 dead, 17 wounded in California shooting; 2 suspects dead*, AP News, (December 3, 2015), https://apnews.com/e5660a0b4ae1436fb2c51354cef8f6db/california-

police-respond-report-active-shooter.

84. Id.
85. Dustin Volz & Mark Hosenball, *FBI director says investigators unable to unlock San Bernardino shooter's phone content*, Reuters, (February 9, 2016), https://www.reuters.com/article/us-california-shooting-encryption-idUSKCN0VI22A.
86. Jenna McLaughlin, *NSA Looking To Exploit Internet Of Things, Including Biomedical Devices, Official Says*, *The* Intercept_, (June 10, 2016), https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/.
87. Andrew Blankstein, *Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone*, NBC News, (February 16, 2016), https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701.
88. Danny Yadron, *Apple says the FBI is making access demands even China hasn't asked for*, The Guardian, (February 19, 2016), https://www.theguardian.com/technology/2016/feb/19/apple-fbi-encryption-battle-san-bernardino-shooting-syed-farook-iphone.
89. Mike Levine, Jack Date & Jack Cloherty, *DOJ Escalates Battle With Apple Over San Bernardino Shooter's Phone*, ABC News, (February 19, 2016), https://abcnews.go.com/US/doj-escalates-battle-apple-san-bernardino-shooters-phone/story?id=37056775.
90. Paresh Dave, *Apple and feds reveal San Bernardino shooter's iCloud password was reset hours after attack*, Los Angeles Times, (February 19, 2016), http://www.latimes.com/business/la-fi-tn-apple-fbi-call-20160219-story.html.
91. Joel Rubin, James Queally & Paresh Dave, *FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now*, Los Angeles Times, (March 28, 2016), http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.
92. Brad Heath, *Others sue FBI for info on phone hack of San Bernardino shooter*, USA Today, (September 16, 2016), https://www.usatoday.com/story/news/nation/2016/09/16/usa-today-lawsuit-fbi-iphone-hack-san-bernardino/90477540/.
93. Josh Gerstein, *Judge: FBI can keep cost of iPhone hack secret*, Politico, (October 1, 2017), https://www.politico.com/blogs/under-the-radar/2017/10/01/judge-fbi-need-not-release-cost-of-iphone-hack-243338.
94. Mill, 1859 at 18.
95. Id.
96. Id.
97. Mill. 1859, at 154-155.
98. Id.
99. Id.
100. Id.
101. *Legal Theory Lexicon: Balancing Tests*, *supra*.
102. U.S. Const., Preamble.
103. John Mueller, *Why We Shouldn't Exaggerate the Scale of Terrorism*, Time Magazine, (November 1, 2017), http://time.com/5006353/why-we-shouldnt-exaggerate-the-scale-of-terrorism/.
104. Kevin Townsend, *supra*.
105. Mill, 1859, at 130.
106. Id.
107. Id.
108. *Legal Theory Lexicon: Balancing Tests*, Legal Theory Blog, (August 4, 2013), http://lsolum.typepad.com/legaltheory/2013/08/legal-theory-lexicon-balancing-tests.html.