Installing Backdoors Assists CyberTerrorists

Carl Hewitt

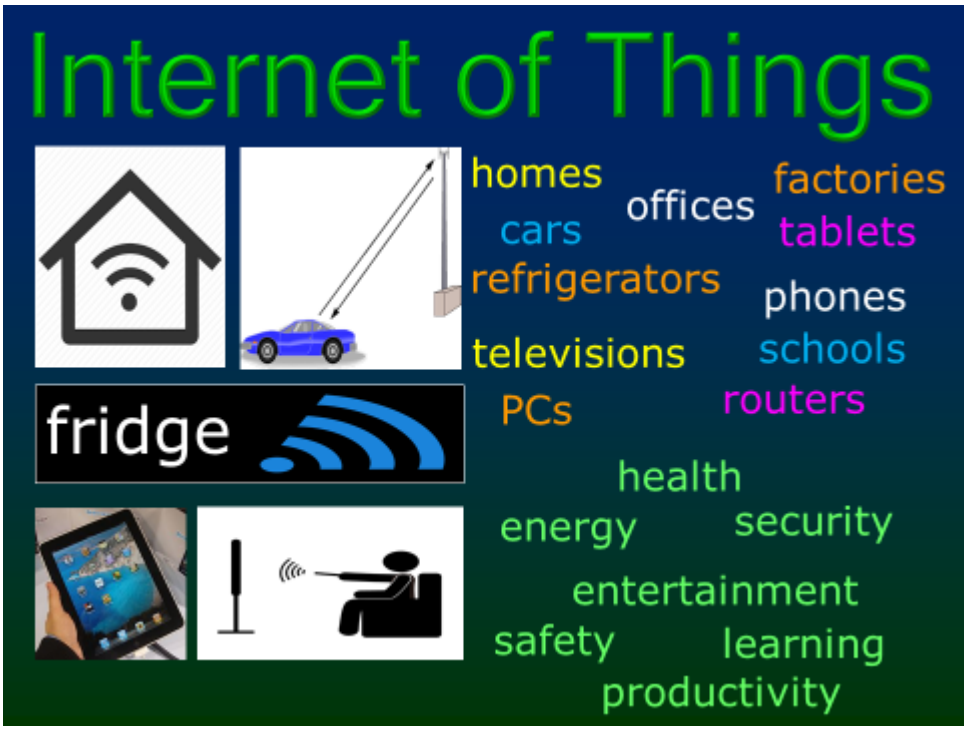
Installing Backdoors Assists CyberTerrorists

"Own your CyberThings" [i]

Carl Hewitt

A government-sponsored crash campaign can dramatically increase the security of Internet of Things (IoT) devices, *e.g.*, cell phones, refrigerators, TVs, PCs, Internet LEDs, *etc*. But security services proposed mandatory backdoors[1] for all IoT are fraught with peril.

The Internet of Things (IoT) is becoming pervasive in all aspects of life including personal, corporate, government, and social.



A CyberThing is a physical or electronic artifact of Internet systems, e.g., light fixture, email, refrigerator, voice mail, cellphone, SMS, electronic door lock, *etc*. on the Internet.

[i] service mark of nonprofit foundation Standard IoT™

DataCenterism (*i.e.*, a system in which *all* electronic information is accessible in datacenters) is becoming the standard business model of the Internet. (Of course, encrypted information is not accessible unless the corresponding decryption key is accessible.)

In due course, it seems inevitable that governments in most countries will obtain (as each cyberattack increases pressure to react) bulk access to all information in datacenters with pipes to government surveillance datacenters in order to speed and coordinate government security efforts.

- **DataCenterism** is a system in which *all* electronic information is accessible in datacenters.
- **CyberTotalism** is a system in which all electronic information is accessible in corporate and government datacenters with *total access* by the government.
- **Sensitive information** is nonpublic information whose revelation can potentially harm a citizen, *e.g.*, medical (including psychiatric), legal, financial, sexual, political, religious, *etc*.
- **CyberLocalism** is a system in which a citizen's Internet of Things information is stored locally in their own equipment–*the antithesis of both Datacenterism and CyberTotalism.*

Consequently, Datacenterism inevitably progresses towards *CyberTotalism*, a system in which all electronic information is accessible in corporate and government datacenters with *total access* by the government to its citizens' information.

To facilitate faster and more comprehensive security operations, governments want to use corporate information mining tools in corporate datacenters for security purposes (perhaps with some direct costs reimbursed by the government) thereby making their engineers and executives *increasingly complicit in mass surveillance*. Furthermore, businesses can be harmed by the following developments:

- their inability to change datacenter operations because it would disrupt government surveillance
- the enforcement of uniformity of datacenter operations across companies (to the competitive disadvantage of the companies) because of government requirements for standardized surveillance operations across companies.

Corporations need to come to better understand that sensitive citizen information is not always a corporate asset and instead can be a toxic corporate liability.

Corporate datacenters are best used for statistical operations that do not have sensitive personal information. Those with large amounts of sensitive citizen information (e.g. financial and medical) will be highly regulated..

Fortunately, there is an alternative to CyberTotalism:

CyberLocalism is a system in which a citizen's sensitive information is stored locally in on their own equipment (without backdoors) – *the antithesis of both Datacenterism and CyberTotalism*.

Sensitive information is nonpublic information whose revelation can potentially harm a citizen, *e.g*., medical (including psychiatric), legal, financial, sexual, political, religious, *etc*. For example:

- The FBI tapped into conversations between Robert Oppenheimer and his lawyer during the hearing designed to humiliate him by having his security clearance removed in order to punish him for some of his political views.
- The FBI COINTELPRO program persecuted thousands, *e.g*., gay people, almost all groups protesting the Vietnam War, and organizations and individuals associated with the women's rights movement. For example, the FBI recorded conversations between Martin Luther King and his mistresses and then used the information to blackmail him suggesting that he commit suicide in order to avoid exposure.
- Maintaining files on millions of East Germans, the Stasi secretly ruined the lives of tens of thousands.[3]
- The US Senate Select Committee *Final Report on Intelligence Activities and the Rights of Americans* [1976] documented Constitutionally illegal surveillance by US Presidents, which it later turned out spanned all presidents from FDR to Nixon, including the following [summarized in Wikipedia] (with government deception continuing to the present):[4]
    - President Roosevelt asked the FBI to put in its files the names of citizens sending telegrams to the White House opposing his "national defense" policy and supporting Col. Charles Lindbergh.
    - President Truman received inside information on a former Roosevelt aide's efforts to influence his appointments, labor union negotiating plans, and the publishing plans of journalists.
    - President Eisenhower received reports on purely political and social contacts with foreign officials by Bernard Baruch, Eleanor Roosevelt, and Supreme Court Justice William O. Douglas.
    - The Kennedy administration had the FBI wiretap a congressional staff member, three executive officials, a lobbyist, and a Washington law firm. US Attorney General Robert F. Kennedy received the fruits of an FBI wiretap on Martin Luther King, Jr. and an electronic listening device targeting a congressman, both of which yielded information of a political nature.
    - President Johnson asked the FBI to conduct "name checks" of his critics and members of the staff of his 1964 opponent, Senator Barry Goldwater. He also requested purely political intelligence on his critics in the Senate, and received extensive intelligence reports on political activity at the 1964 Democratic Convention from FBI electronic surveillance.
    - President Nixon authorized a program of wiretaps which produced for the White House purely political or personal information unrelated to national security, including information about a Supreme Court Justice.

A citizen's information system (embedded in home modems, routers, car, gateways, large screen displays, audio-visual systems, computers, refrigerators, stoves, climate control systems, washer/dryers, *etc*.) can hold the most sensitive of a citizen's information where it can be integrated with other sensitive information as well as information from the following:

- other information from the citizen's IoT
- other parties including datacenters.

CyberLocalism has the following advantages over Datacenterism:

- **Lower communications cost** because it is not necessary to always communicate with datacenters
- **Faster response** because local communication can be faster than always interacting with datacenters, which might be slow to respond
- **Better coordination of IoT** because it can be difficult to get datacenters of competing companies to coordinate concerning the interoperation of a citizen's IoT devices
- **Greater reliability** because communication with datacenters might be interrupted
- **Better protection of a citizen's sensitive information** because it is not always available in datacenters.

The widespread adoption of CyberLocalism will depend on the development of new Internet business models. Please see the appendix of this paper for discussion.

The current default security strategy has not worked, namely, "beating up on personnel to improve security until the public outcry subsides."

CyberLocalism requires greater security of citizens' Internet of Things devices because state-sponsored intruders can hack into almost every citizen's personal cellphone, computer, tablet, etc. on the Internet.

To achieve adequate security, CyberLocalism needs the following:

- **Strong personal authentication**, *e.g.*, using (3D) continuous interactive bio-authentication instead of passwords
- **Strong, ubiquitous public key authentication** so that it can be verified to whom a public key corresponds. Often this authentication can be performed by local bank offices, *etc.* that publish online multi-national directories of public keys in a network of mistrust. Individual citizens can have their own directories of public keys that are used to automatically and invisibly securely communicate with others.

  Many citizens will have more than one authenticated public key, which can be authenticated with various levels of security.
- **Public keys for IoT ownership** so that an IoT device has both:
  - a public key of its owner, which is installed when ownership is transferred
  - its own unique public/private key pair, which is created internally when acquired by the first owner.

  An owner can communicate securely with a device by encrypting information using the device's public key. (For efficiency reasons, most communication will actually be performed using symmetric keys encrypted/signed by public keys.) A device takes instructions only from its owner and is allowed to communicate with the external world only through the information coordination system of its owner. The nonprofit Standard IoT Foundation is working to develop standards based on the Actor Model of computation that provide for interoperation among existing and emerging consortium and proprietary corporate IoT standards.

- **Hardware architecture security** to help cope with the complexity of software systems that can never be made highly secure without hardware assistance including the following:
    - *RAM-processor package encryption* (*i.e.* all traffic between a processor package and RAM is encrypted using a uniquely generated key when a package is powered up and which is invisible to all software) to protect an app (*i.e.* a user application, which is technically a process) from the following:
        - operating systems and hypervisors
        - other apps
        - other equipment, e.g., baseband processors, disk controllers, and USB controllers.
    - *Every-word-tagged architecture* to protect an Actor in an app from other Actors by using a tag on each word of memory that controls how the memory can be used. Each Actor is protected from reading and/or writing by other Actors in its process. Actors can interact only by sending a message to the unforgeable address of another Actor. Existing software (e.g., operating systems, browsers, mail systems) will need to be upgraded to use tags.

Because of impending security improvements, it will become extremely difficult even for state-sponsored intruders to easily hack into IoT endpoints.

The looming prospect of not being able to easily hack into IoT devices undetected (perhaps with some kind of court order) has alarmed some security services, prompting them to demand mandatory backdoors be installed in all IoT equipment within their jurisdiction.

IoT Backdoors

On March 2, 2015, President Obama complained about a government attempt to require backdoors in companies' products saying:

> *"As you might imagine tech companies are not going to be willing to do that... I don't think there is any U.S. or European firm, any international firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government."*[5]

If the US and EU adopt auditing against backdoors, then auditing will rapidly spread to the rest of the world, which is very much in their long-term security interests.

However, FBI Director James Comey [speech on October 17, 2014] and NSA Director Mike Rogers have proposed that CALEA[8] be expanded so that every cell phone, personal computer and any other network-enabled products and services that operate in the US must have a backdoor in order that the US government can hack in undetected with the approval of US courts.[9]

Rogers clamed: "Building it [secure backdoor command and control system] is technically feasible."[10] However, he admitted that if the FBI/NSA mandatory backdoor proposal is adopted, then it will be necessary to "work through" arrangements with other governments to have their own backdoors and any consequential restrictions on Internet interconnectivity and international trade of IoT products.

Highly secure backdoors can use the equivalent of a different public key on each device. Control of private keys for backdoors can use means similar to the ones currently used in nuclear command, control, and communication systems, which have had many problems.[11] However, at an expense comparable to nuclear command and control systems, it would be possible to create a system for protecting the keys of a backdoor system that is highly secure against outside attackers and even against a small number of inside conspirators. Such a system can use multiple command centers with divided keys. In other words, according to Mike Rogers (Director of NSA), such system would require "*multiple locks. Big locks*."[12] Even with such a system, it is possible that, later on, some backdoors of older IoT devices could be compromised by criminals and state-sponsored attackers.

Adopting the NSA/FBI mandatory backdoor proposal for all IoT (including devices that electronically communicate with IoT) can have the following effects:

- Influence countries to require that IoT products sold in a country will have to be audited against backdoors available to *other* countries. It is technically much easier to audit against *all* backdoors that to audit against other countries being able to exploit an *already installed* backdoor.
- Increase the danger of preemptive cyberwar[13] because of potential vulnerabilities in the many government backdoor implementations.[14]
- Decrease the competitiveness of US manufacturers in the market of the IoT, which will include almost *everything*.[15]
- Enormously increase the power of government security monitors.[16] Mass surveillance by the US Government has been extraordinary effective in taking out opponent leadership in Afghanistan, Pakistan, Somalia, Yemen,

> *etc*.[17] However, the extreme effectiveness demonstrates how dangerous surveillance technology has become to civil liberties.[18] As pointed out previously in this article, mass surveillance has a long history of being used to terrorize and intimidate political opponents, unpopular minorities, and the populace in general. State terrorists achieve political objectives by creating a general climate of fear. For example, J. Edgar Hoover (FBI), Joe McCarthy (US Senate Permanent Subcommittee on Investigations), Erich Mielke (Stasi)[18], *etc*. terrorized citizens of their countries. Cyberterrorists can exploit the immense power of IoT backdoors to create mass terror on a scale that was heretofore unimaginable.[19]

In fact, the NSA/FBI mandatory backdoor proposal has *already* increased mistrust by foreign governments and citizens alike, with the consequence[20] that companies will be required to hire their own independent cyberauditors and/or submit to cyberaudits by foreign governments to ensure that exports do not have backdoors accessible by the US government.[21] Likewise, every other government will require that IoT sold in their country do not have backdoors accessible to other governments.

Mandatory backdoors will mean that security services of each country will surveil citizens in their own country and perhaps swap surveillance information with other countries.

Conclusion

> *The only thing necessary for the triumph of evil is for good men to do nothing*.
> Edmund Burke

Future exports of U.S. companies will need to be certified by corporate officers and independently audited not to have backdoors available to the U.S. government.

An IoT Security Commission (ISC) needs to be established with the following charter:

1. **Jurisdiction:** ISC will have jurisdiction over all providers of IoT equipment in the US. Every IoT device will be required to be audited by mechanisms determined by ISC, *e.g.*, operational bi-simulation against a publicly available operational specification overview.
2. **Quarterly Corporate Security Report:** ISC will enforce that at end of each quarter, a corporate security report must be signed by the corporate officers of a covered company, which must specify either
   i. no evidence for the existence of a backdoor was found in any of the company's IoT products or that
   ii. evidence that was found for the existence of backdoors and the measures that were taken to remove backdoors from any products that were shipped and to prevent re-occurrence.
3. **Oversight:** ISC will provide independent oversight of public security accounting firms providing cyberaudit services ("*cyberauditors*") that will:
   - register cyberauditors
   - define specific processes and procedures for compliance cyberaudits
   - inspect and police cyberaudit conduct and quality control
   - restrict cyberauditing companies from providing non-audit services (*e.g.*, consulting) for the same clients.
   - enforce compliance with specific legal mandates, *e.g.*, the use of RAM-processor encryption and every-word-tagged architectures.

Using mechanisms outlined in this article, the US can immediately launch a crash program to secure IoT devices (including corporate, citizen, utility, and government) thereby making them dramatically more secure.

Acknowledgements

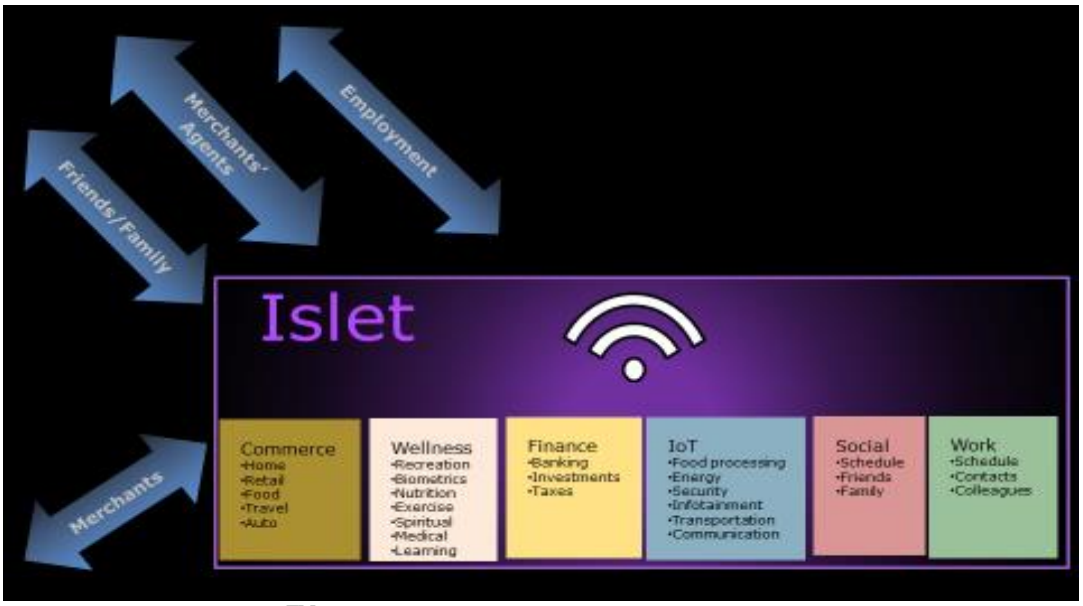
This article has greatly benefited from detailed critiques and organizational suggestions of Alan Karp, editorial suggestions of Dennis Allison, comments by Chip Morningstar, and a suggestion of Ron Rivest. John Dalton provided design and editorial consulting.

The following video covers material in this article:
Actors for CyberThings. https://youtu.be/DNbJY333vUs

***Appendix*: New Internet Business Model**

CyberLocalism will never come to fruition unless it is supported by a business model that is more efficient and effective than the currently popular system of datacenterism.

An **Islet** provides information coordination and interaction services for a citizen's sensitive information.



Islet™ Information Coordination and Interaction

An Islet can provide additional capabilities that are not currently available for coordinating and interacting with cyberthings:[22]

- **Commerce**: home, retail, food, travel, auto, *etc.*
- **Wellness:** recreation, biometrics, nutrition, exercise, spirituality, medical, learning, *etc.*
- **Finance:** banking, investments, taxes, *etc.*
- **IoT:** food management, security, energy management, infotainment, transportation, communication, *etc.*[24]
- **Social:** schedule, friends, family, *etc.*
- **Work:** contacts, schedule, colleagues, *etc.*

Inconsistency robustness[23] is information system performance in the face of continual, pervasive inconsistencies.

Inconsistency robustness is both an observed phenomenon and a desired feature.

Coordination includes all kinds of digital information for individuals, groups, and organizations so their information usefully links together. This coordination can include calendars and to-do lists, communications (including email, SMS, phone mail), presence information (including who else is in the neighborhood), physical (including GPS recordings), psychological (including facial expression, heart rate, voice stress) and social (including family, friends, team mates, and colleagues), maps (including firms, points of interest, traffic, parking, and weather), events (including alerts and status), documents (including

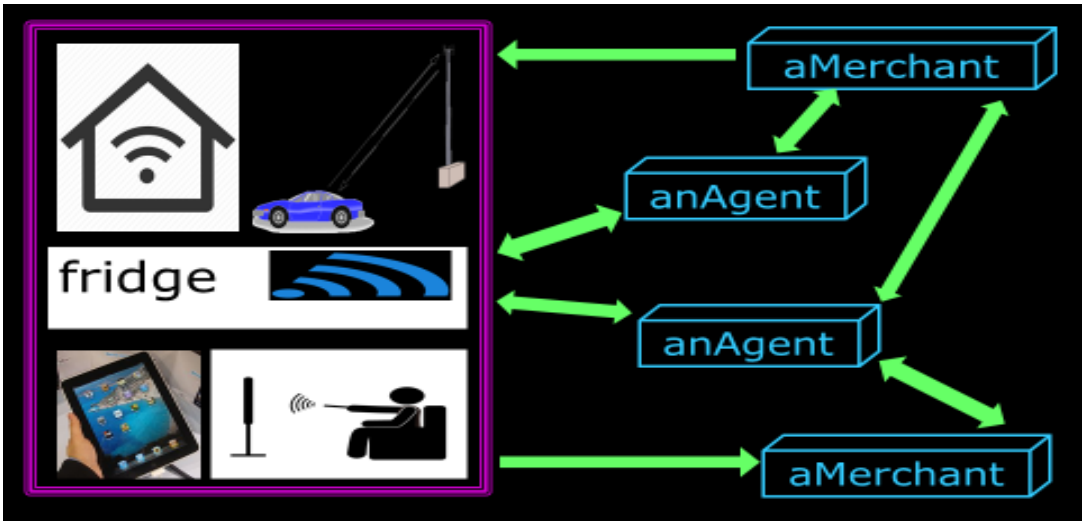
presentations, spreadsheets, proposals, job applications, health records, photos, videos, gift lists, memos, purchasing, contracts, articles), contacts (including social graphs and reputation), purchasing information (including store purchases, web purchases, GPS and phone records, and buying and travel habits), government information (including licenses, taxes, and rulings), and search results (including rankings and ratings).

Classical logic (the basis for relational databases) is *not* a suitable foundation for information coordination because a single (hidden) inconsistency can cause incorrect reasoning. Fortunately, recent advances in the development of inconsistency-robust information systems technology can be used to more safely reason about pervasively inconsistent information (even without knowing which pieces of information might be inconsistent).[25]

Of course, all of the convenience that is currently available must also be available using an Islet:

- An Islet can access the Internet to provide scalable search, retrieval, and collaboration using commercial datacenters in cooperation with other citizens' equipment.
- Islet information can be backed up elsewhere automatically encrypted using the citizen's public keys, *e.g.*, in commercial datacenters and distributed on other citizens' equipment.
- A citizen can share Islet information that they select with others (automatically encrypted with the public keys of other parties so that it be read only by the intended recipient).

Attempting to provide cyberthing coordination and interaction services by patching together datacenter services from fierce competitors is much more difficult, *e.g.*, consider Amazon, Carrier, Cisco, Dell, Electrolux, Facebook, GE, Google, Haier, HP, Huawei, IBM, Lenovo, LG, Microsoft, Panasonic, Samsung, Whirlpool, *etc*.



Islet Coordinating with Merchants

Fortunately, recent advances in the development of inconsistency-robust information systems technology can be used to facilitate new business implementations that are more *effective*, *pervasive*, and *profitable* by improving interactions among consumers and merchants because:

- Consumers will no longer be continually hassled by intrusive unwanted advertisements. Instead, an Islet running on a consumer's equipment can provide the ability to seek and help evaluate appropriate offers from commerce agents for their purchases. Commerce agents can earn commissions and fees from merchants when a citizen uses the referrals.
- Merchants will no longer be burdened by having to pay for *grossly inefficient* advertising that annoys potential customers. Instead, businesses can provide their information to commerce agents that aggregate and package it for a citizen's' Islet to be used in evaluating offers. Again, commerce agents can earn commissions and fees from merchants from referrals.

References

[1] A **backdoor** is means by which a cyber device can provide information and control about the users of a device
  - to parties that were not specifically enumerated
  - concerning kinds of information and control that were not specifically described
  - that was not specifically authorized by users of the device.

[2] Lee Fang. *How Big Business Is Helping Expand NSA Surveillance, Snowden Be Damned*. The Intercept. April 1, 2015.

[3] Florian Henckel von Donnersmarck. *The Lives of Others*. Wiedemann & Berg, et. al. 2006.

[4] John Gilmore and Mike Wiser. *Secrets, Politics and Torture*. PBS Frontline. May 19, 2015.

[5] Mike Burnside, Dave Clarke, T. Mills, A. Maywah, S. Davadas, and Ronald Rivest. *Proxy-Based Security Protocols in Networked Mobile Devices*. SAC'2002.

[6] Carl Hewitt. *Actor Model of Computation.* in "Inconsistency Robustness" College Publications. 2015.

[7] Jeff Mason. *Obama sharply criticizes China's plans for new technology rules*. Reuters. March 2, 2015.

[8] EFF. *Response to FBI Director Comey's Speech on Encryption.* October 17, 2014].

Here's the relevant part of CALEA that Comey wants to effectively undo:

"USC 1002(b)(3): A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."

Also from the CALEA legislative history:

"Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. ... Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access ... Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption

within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, section 2602 protects the right to use encryption."

[9] Jeremy Scahill and Josh Begley. *The CIA Campaign to Steal Apple's Secrets*. The Intercept. March 10, 2015.

[10] Mike Rogers. *National Security Agency Director Mike Rogers on Cybersecurity.* CSPAN. February 23, 2015.

[11] Eric Schlosser. *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*. Penguin Books. 2014.

[12] Ellen Nakashima and Barton Gellman. *As encryption spreads, U.S. grapples with clash between privacy, security*. Washington Post. April 10, 2015.

[13] Shane Harris. *@War: The Rise of the Military-Internet Complex.* Eamon Dolan/Houghton Mifflin Harcourt. Boston, MA, 2014.

[14] Bill Marczak, et. al.. *China's Great Cannon*. University of Toronto. April 10, 2015.

[15] James Staten. *The Cost of PRISM Will Be Larger Than ITIF Projects* James Staten's Blog at Forrester Research. August 14, 2013.

[16] Robert Scheer. *They Know Everything About You* YouTube. Town Hall Seattle. March 16, 2015. Peninsula Peace and Justice Center. March 27, 2015.

[17] Barack Obama. *Al Qaeda Has Been Decimated* YouTube. November 1, 2012. Long-term effects of the Obama administration's assassination campaign are unknown.

[18] Anna Funder. *Stasiland: Stories from Behind the Berlin Wall*. Harper. 2011

[19] Michael Glennnon. *National Security and Double Govenment* Harvard National Security Journal. Vol. 5. 2014.

[20] Peter Swire and Kenesa Ahmad. *Encryption and Globalization.* Columbia Science and Technology Law Review. Vol. 23. 2012.

[21] Li Dandan. *Apple expresses willingness to accept the Chinese domestic network security review*. Beijing News. January 21, 2015.

[22] Carl Hewitt. *Actors for CyberThings.* YouTube. March 23, 2015.

[23] Carl Hewitt and John Woods assisted by Jane Spurr, Editors. *Inconsistency Robustness*. College Publications. 2015.

[24] Edward Lee. *Swarm Boxes*. SwarmLab UC Berkeley. March 19, 2015

[25] Carl Hewitt. *Formalizing common sense reasoning for scalable inconsistency-robust information coordination using Direct Logic™ Reasoning and the Actor Model*. in "Inconsistency Robustness" College Publications. 2015.