Distributed Public Recording

Carl Hewitt

Distributed Public Recording

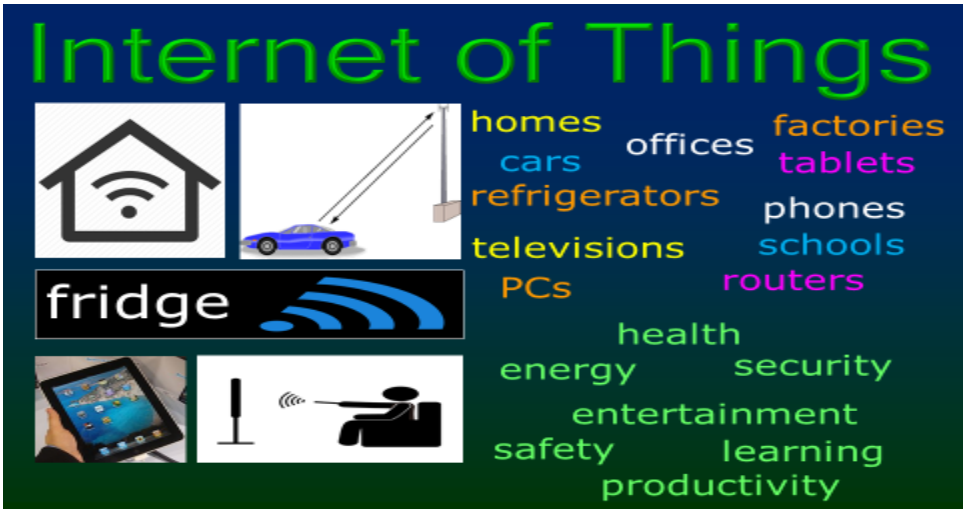
Providing Security Without the Risks of Mandatory Backdoors

Carl Hewitt

Distributed Public Recording **(DPR) is a system in which distributed public and private organizations (e.g., stores, restaurants, sports events, parks, theaters, *etc.*) keep electronic records (that can be accessed only with a court subpoena and otherwise must be completely erased after two years) of all activity that takes place in public places including tracking automobiles, cell phones, humans (using facial recognition), *etc.* and all financial transactions. Advanced Inconsistency Robust[10] information technology can be a very powerful tool for catching criminals using DPR, which is a less risky to security than requiring mandatory backdoors[i] for all Internet of Things (IoT) devices, *e.g.*, cell phones, refrigerators, TVs, PCs, Internet LEDs, *etc.***

Preliminary to discussing Distributed Public Recording (DPR), this article presents background on IoT security issues including the role played by datacenters before returning to DPR at the end.

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



[i] 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.

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."*[17]

If the US and EU adopt auditing against backdoors, then auditing can 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[21] 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 to provide security services with the ability to access and control the device undetected by the user with the assent of US courts.[22]

IoT Backdoors

However, Rogers 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.

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

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.[1][24] However, using the equivalent of a different public key on each device, 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 by using multiple command centers with split keys. In other words, according to Rogers, such system would require "*multiple locks. Big locks*." 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 mandatory backdoor proposal that it must be possible for security services to secretly access and control each individual IoT device can make it very difficult to prevent security services from accessing and controlling large numbers of devices and abusing their surveillance capabilities.

The NSA/FBI mandatory backdoor proposal for all IoT (including devices that electronically communicate with IoT) can influence countries to require that IoT products sold in a country must 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. Mandatory backdoors can increase the risk of preemptive cyberwar[8] because of potential vulnerabilities in the many government backdoor implementations.[16] Also, mandatory backdoors can enormously increase the power of government security monitors.[7]

Furthermore, mandatory backdoors can decrease the competitiveness[20] of US manufacturers in the market of the IoT, which will include almost *everything*. As a result of the revelations of NSA foreign surveillance, it has become clear that the U.S. tech industry as a whole, not just the cloud computing sector, has under-performed[3] with informed estimates of losses of US companies now north of $180B and still climbing.[20] In short, foreign customers are shunning U.S. companies.[3]

In fact, the NSA/FBI mandatory backdoor proposal has *already* increased mistrust by foreign governments and citizens alike, with the consequence[4] that companies can 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.[25] Likewise, every other government can require that IoT sold in their country do not have backdoors accessible to other governments.

Future exports of U.S. companies can be required to be certified by corporate officers and independently audited not to have backdoors available to the U.S. government. An IoT Security Commission (ISC) could to be established with jurisdiction over all providers of IoT equipment in the US:

> Every IoT device would be required to be audited by mechanisms determined by ISC, *e.g.*, operational bi-simulation against a publicly available operational specification

overview. At end of each quarter, a corporate security report would be required signed by the corporate officers of a covered company, which must specify either that no evidence for the existence of a backdoor was found in any of the company's IoT products or that 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. ISC would provide independent oversight of public security accounting firms providing cyberaudit services ("*cyberauditors*") that 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 and enforce compliance with specific legal mandates, *e.g.*, the use of RAM-processor encryption and every-word-tagged architectures.

Mass surveillance by the US Government has been extraordinary effective in taking out opponent leadership in Afghanistan, Pakistan, Somalia, Yemen, *etc*.[18] The Chinese security services have accessed US computer systems to collect sensitive information on millions of Americans.[15] Under the likes of the National Recognizance Organization slogan "*Nothing is beyond our reach*", US security services have likewise have conducted extensive surveillance, access, and control of information systems in China.

The extreme effectiveness of mass surveillance (in Afghanistan, *etc.*) demonstrates how risky government surveillance, access, and control technology have become to civil liberties.

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)[5], *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.

Following the US Senate committee investigation into domestic spying by the U.S. intelligence community, Committee Chairman Frank Church made the following prophetic statement:

> "[The NSA's] *capability at any time could be turned around on the American people, and no American would have any privacy left, such* [is] *the capability to monitor everything: telephone conversations, telegrams, it doesn't matter***.**" There is, Church said, "*tremendous potential for abuse*" should the NSA "*turn its awesome technology against domestic communications.*"

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, security services in many countries can 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 tends to progress 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.[23]

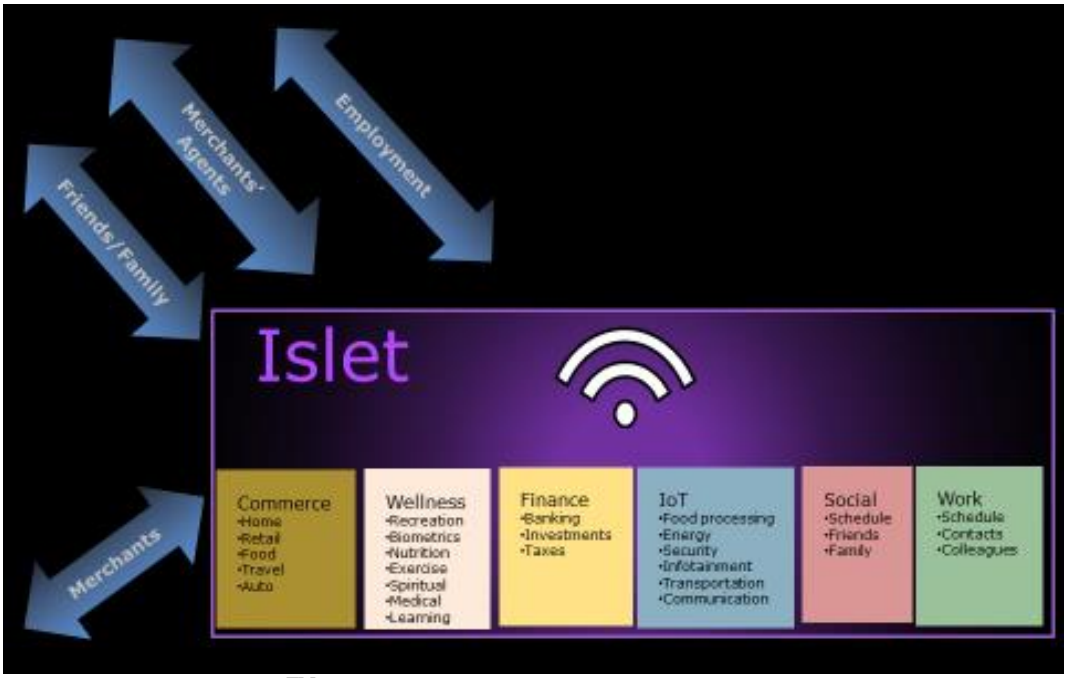
To facilitate faster and more comprehensive security operations, governments want to use corporate information mining tools in corporate datacenters for security purposes (perhaps with some direct costs reimbursed by the government) thereby making their engineers and executives *increasingly complicit in mass surveillance*. Furthermore, businesses can be harmed by their inability to change datacenter operations because it would disrupt government surveillance. Government security services can enforce uniformity of datacenter operations across companies to increase the effectiveness and efficiency of their surveillance operations at the cost of inhibiting innovation and flexibility of company operations.

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

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*.

CyberLocalism has important advantages over Datacenterism including 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, and better protection of a citizen's sensitive information because it is not always available in datacenters.

CyberLocalism might 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.



Islet™ Information Coordination and Interaction

An Islet[ii] can provide additional capabilities that are not currently available for coordinating and interacting with cyberthings[iii] including *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.*)[2], *Social* (schedule, friends, family, *etc.*),. and *Work* (contacts, schedule, colleagues, *etc.*)*:* [13]

> Every IoT device would be required to be audited by mechanisms determined by ISC, *e.g.*, operational bi-simulation against a publicly available operational specification overview. At end of each quarter, a corporate security report would be required signed by the corporate officers of a covered company, which must specify either that no evidence for the existence of a backdoor was found in any of the company's IoT products or that 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. ISC would provide independent oversight of public security accounting firms providing cyberaudit services ("*cyberauditors*") that register cyberauditors, define specific processes and procedures for compliance

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

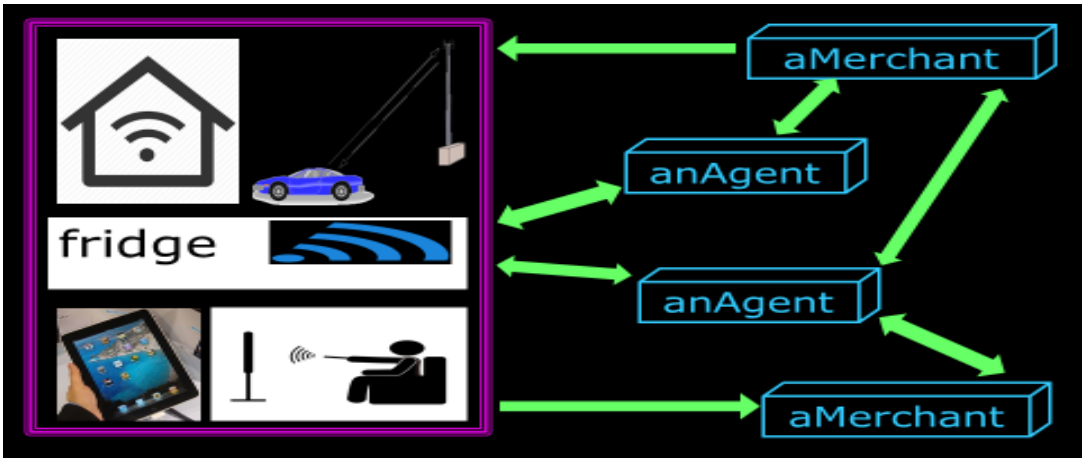
[iii] A *CyberThing* is a physical or electronic artifact of Internet systems, e.g., light fixture, email, refrigerator, voice mail, cellphone, SMS, electronic door lock, *etc*. on the Internet.

cyberaudits, inspect and police cyberaudit conduct and quality control, restrict cyberauditing companies from providing non-audit services (*e.g.*, consulting) for the same clients and enforce compliance with specific legal mandates, *e.g.*, the use of RAM-processor encryption and every-word-tagged architectures.

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[iv] information systems technology can be used to more safely reason about pervasively inconsistent information (even without knowing which pieces of information might be inconsistent).[11]

Of course, all of the convenience that is currently available must also be available so that An Islet can access the Internet to provide scalable search, retrieval, and collaboration using commercial datacenters in cooperation with other citizens' equipment. Also, 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. Furthermore, 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.[v]



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

[iv] *Inconsistency robustness*[10] is information system performance in the face of continual, pervasive inconsistencies.

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

[v] Amazon, Apple, Carrier, Cisco, Dell, Electrolux, Facebook, GE, Google, Haier, HP, Huawei, IBM, Intel, Lenovo, LG, Microsoft, Panasonic, Samsung, Whirlpool, *etc.*

because consumers would 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. Also, merchants would 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.

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. Also, 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. Furthermore, 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. Likewise, maintaining files on millions of East Germans, the Stasi secretly ruined the lives of tens of thousands.[9]

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 owing [summarized in Wikipedia] (with government deception continuing to the present):[6]

> 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 while 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 and 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.

CyberLocalism requires greater security of citizens' Internet of Things devices because currently state-sponsored intruders can access and control almost any citizen's personal

cellphone, computer, tablet, etc. on the Internet even if the device is turned off. To achieve adequate security, CyberLocalism has a number of requirements[12] including strong personal authentication, *e.g.*, using (3D) continuous interactive bio-authentication instead of passwords and 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 can have more than one authenticated public key, which can be authenticated with various levels of security.

Public keys for IoT ownership are required 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 can 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.

Increased hardware architecture security is needed to help cope with the complexity of software systems that can never be made highly secure without hardware assistance.

> Needed hardware extensions include 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 operating systems and hypervisors, other apps, and other equipment, e.g., baseband processors, disk controllers, and USB controllers. Also, Every-word-tagged architecture is needed 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 implementations (e.g., operating systems, browsers, data bases, mail systems, *etc.*) will need to be upgraded to use tags.

Because of impending security improvements, it can become extremely difficult even for state-sponsored intruders to easily access and control IoT devices, e.g., cell phones, personal computers, refrigerators, TVs, *etc.*

Conclusion

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

The current capability of the US government to conduct mass surveillance on everyone in the world is coming to an end[19] with a speed depending in part on how fast the security measures presented in this article are deployed.

Security services have proposed mandatory backdoors for all IoT. Mandatory backdoors mean that security services of each country surveil citizens in their own country and perhaps swap surveillance information with other countries. Adopting the mandatory backdoor proposal is fraught with peril because making it possible for security services to secretly access and control each individual IoT device can make it very difficult to prevent security services from accessing and controlling large numbers of devices thereby abusing their surveillance capabilities. Going forward, mandatory backdoors can be used by a government to tightly control its own populace, which would constitute a fundamental change in social relationships with unknown but enormous consequences.

Mandatory standardization of datacenter operations for surveillance could tremendously reduce the power and resources of multinational Internet companies[vi] versus governments of nation states because these companies would not be able to operate internationally because no country would trust sensitive information of its citizens to be stored in datacenters accessible by security services of other countries. One possible outcome could be for the multi-nationals to become separate corporations domiciled in each nation (for security reasons) to serve just that nation.

On August 1, 2007, then Senator Barack Obama called for an alternative to oppressive mass surveillance:

> *That means no more illegal wiretapping of American citizens. No more national security letters to spy on citizens who are not suspected of a crime. No more tracking of citizens who do no more than protest a misguided war.*

Distributed Public Recording (DPR) inhibits mass surveillance by requiring a court subpoena to access information recorded by distributed parties (*e.g.*, stores, restaurants, sports events, parks, theaters, *etc*.) thereby making mass surveillance more costly, both politically and economically. Advanced Inconsistency Robust[10] information technology can be a very powerful tool for catching criminals using DPR because it can provide principled methods and technology for processing large amounts of pervasively inconsistent information.

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 suggestions of Ron Rivest and Peter Neumann. John Dalton provided design and editorial consulting.

[vi] Alibaba, Amazon, Apple, Cisco, Facebook, Google, HP, IBM, Intel, LG, Microsoft, Panasonic, Samsung, Yahoo, *etc*.

The author's Erlang keynote address *Actors for CyberThings* covers some of the material in this video.[13]

References

[1] Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh. Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller and Bruce Schneier. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* World Wide Web Journal. O'Reilly. Vol. 2, No. 3. 1997.

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

[3] Daniel Castro and Alan McQuinn. *Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness* Information Technology and Innovation Foundation. June 9. 2015.

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

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

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

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

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

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

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

[11] 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.

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

[13] Carl Hewitt. *Actors for CyberThings.* Erlang Keynote. YouTube. March 23, 2015.

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

[15] Ellen Nakashima. *With a series of major hacks, China builds a database on Americans.* Washington Post. June 5, 2015.

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

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

[18] Barack Obama. *Al Qaeda Has Been Decimated* YouTube. November 1, 2012. Long-term effects of the Obama administration's assassination campaign (and attendant killing of innocents) are unknown.

[19] Pierluigi Paganini. *The FBI is not able to monitor ISIS's encrypted communications.* June 4, 2015.

[20] Salvador Rodriguez. *NSA 'Equation' Fallout: Experts Say Damage To US Tech Firms Could Top $180B* International Business Times, February 15, 2015.

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

[22] Jeremy Scahill and Josh Begley. *The CIA Campaign to Steal Apple's Secrets*. The Intercept. March 10, 2015.
[23] Robert Scheer. *They Know Everything About You: How Data-Collecting Corporations and Snooping Government Agencies Are Destroying Democracy* Nation Books. 2015.
[24] Eric Schlosser. *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*. Penguin Books. 2014.
[25] Peter Swire and Kenesa Ahmad. *Encryption and Globalization.* Columbia Science and Technology Law Review. Vol. 23. 2012.