Security without IoT Mandatory Backdoors

Carl Hewitt

▶ **To cite this version:**

Carl Hewitt. Security without IoT Mandatory Backdoors: Using Distributed Encrypted Public Recording to Catch & Prosecure Criminals. 2016. hal-01152495v12

HAL Id: hal-01152495

https://hal.science/hal-01152495v12

Preprint submitted on 29 Feb 2016 (v12), last revised 14 Jun 2016 (v14)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

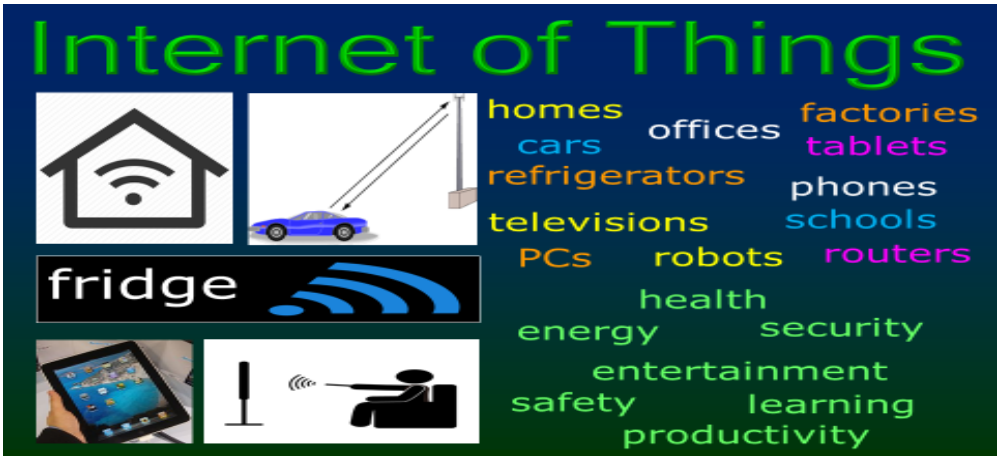
Security without IoT Mandatory Backdoors

Using Distributed Encrypted Public Recording to Catch & Prosecute Criminals

Our greatest enemy is our own apathy.
Bill Mullinax

Carl Hewitt
Board Chair of Standard IoT™ Foundation
https://plus.google.com/+CarlHewitt-StandardIoT/

The Internet of Things (IoT[i]) is becoming pervasive in all aspects of life including personal, corporate, government, and social. Adopting IoT mandatory backdoors[ii] ultimately means that security agencies of each country surveil IoT in their own country and perhaps swap surveillance information with other countries.[11][30][32] Security agencies have proposed that it must be possible for them to secretly access and take control of any individual IoT device. However adopting their proposal would make it very difficult to prevent them from accessing and controlling large numbers of devices and abusing their surveillance capabilities.[9][10][11][30][32] Also, adopting IoT mandatory backdoors would be corrosive to civil liberties because any phone, body-sensor computer network[26], TV, and other IoT device[iii] could be secretly accessed and controlled without any awareness by those present using the device.[9][11][15][32]26] A critical security issue is that after a backdoor has been exercised to take control of a citizen's IoT device without their awareness, the device thereby becomes somewhat *less* secure because of potential vulnerabilities in the new virtualized system used to take control of the device.[0][1][10]][11][15][32]



IoT Ubiquity

[i] *e.g.*, body-sensor computer networks, cell phones, refrigerators, TVs, PCs, Internet LEDs, *etc*.

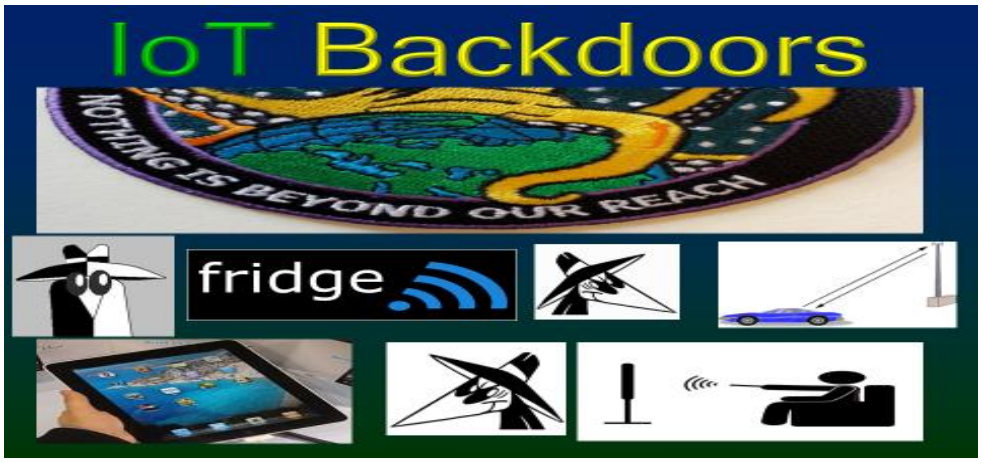
[ii] A *backdoor* is means by which a cyber device can be secretly accessed and controlled by parties that were not specifically enumerated concerning kinds of information and control. that were not specifically described, and that was not specifically authorized by users of the device.

[iii] e.g. in bedrooms, bathrooms, kitchens, and autos

Distributed Encrypted Public Recording (DEPR) is system in which distributediv public and private organizations keep encrypted electronic records of all activity that takes place in outside the homestead including tracking automobiles, cell phones locations, humans (using facial recognition), and all financial transactions. The records can be decrypted only by court warrant using both a key kept by the recording establishment and a key provided by the court. If not court ordered within a time set at recording, the recordings cannot read by anyone (enforced by cryptography using a trans-national distributed Internet time authority). In addition to ensuring that outdated information cannot be decrypted, the trans-national time authority can provide continual statistics on the amount of decrypted information as a deterrent to mass surveillance. Advanced Inconsistency Robust[16] information technology can be a very powerful tool for catching and prosecuting criminals using DEPR. Using DEPR is a less risky to civil liberties than requiring IoT mandatory backdoors for all IoT devices. The DEPR proposal brings out the issue that massive amounts of information are being collected and disseminated with almost no regulation whatsoever. Soon there stands to be even greater collection and dissemination, which will inevitably lead to increasingly severe scandals.

However, IoT devices will require much more powerful integrated security technology than the current patchwork, which can almost always be circumvented by state-sponsored intruders.[4][5][11][16][24][27][32] 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.[15]

FBI Director James Comey's proposed on October 17, 2014 that CALEA be expanded so that every cell phone, body-sensor computer network[26], personal computer and any other network-enabled products and services that operate in the US must have a backdoor to provide security agencies with the ability to secretly access and take control of the device[11][32][39] with the assent of US courts.



Power of IoT Backdoors

[iv] stores, restaurants, sports events, parks, theaters, *etc.*

Mandatory backdoor technology can build on already developed CIA/GCHQ/NSA surveillance technology including QUANTUM, SMURF, TURBINE, TURMOIL, UNITEDRAKE, WARRIOR PRIDE, and VALIDATOR.[11][32] The equivalent of a (preferably unique) public key can be installed by the manufacturer on each a device. The private key can be split held by government authorities of the nation in which the device is to be operated.[38] To secure private keys, means can be used that scale up technology currently used to control keys in nuclear command, control, and communication systems. However, many nations have had numerous security problem with their nuclear weapon controls.[0][33] Using the above technology, it would theoretically 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. A critical security issue is that after a backdoor has been exercised to take over a citizen's IoT device without their awareness, the device thereby becomes somewhat *less* secure because of potential vulnerabilities in the new virtualized system used to take over the device.[11][15][32]

IoT Mandatory Backdoor Proposal[39]

- In order to connect with the public Internet in a country, a legal IoT device must present an interactive certificate (signed by the manufacturer registered with the government) with its backdoor public key.
- All subsequent communications with the public Internet must be signed with an interactive certificate.
- The device must be able to be secretly taken-over & controlled over the Internet using the private key for its backdoor public key.
- Any device that connects to a taken-over device must likewise be able to be taken-over (to subvert use of offline crypto).

The 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.[3][35][37][38][39] 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 risks of both preemptive cyberwar[14] and kinetic responses to cyberattacks because of potential vulnerabilities in the many different government backdoor implementations.[27][35] Also, mandatory backdoors can increase the security risks to military equipment because they might be

IoT mandatory backdoors consequences

- security agencies of each country surveil IoT in their own country and perhaps swap surveillance information with other countries.[11][27][39]
- make it very difficult to prevent security services from accessing and controlling large numbers of devices and abusing their surveillance capabilities[9][10][11][27]
- corrosion of civil liberties because any phone, body-sensor network, computer, and other IoT device (including those in bedrooms, bathrooms, and autos) could be secretly accessed and controlled without any awareness of those present[9][11][15][27]
- massive corruption as a result of sensitive IoT information spreading from local security agencies to their political supervisors[19]
- lower security because after a security service has secretly taken control of an IoT device, the device thereby becomes *less* secure against other potential attackers.[0][1][10][27]

exploited by enemy forces. Furthermore, IoT mandatory backdoors can enormously increase the power of government security agencies.[9][32][36][39][40]

Security agencies have issued secret orders to US corporations allowing security agencies to conduct surveillance worldwide with gag orders that this surveillance not be disclosed.[4][10][13][16][25][30]][34][36][39][40] The resulting mass surveillance of foreigners has caused US tech industry as a whole, not just the cloud computing sector, to under-perform with losses north of $180B and still climbing.[3][30]] "*In short, foreign customers are shunning U.S. companies*."[4] These losses would be increased tenfold if they spread to manufacturers that include IoT connected to their datacenters, which stands to include almost *everything*.

Auditing foreign-domiciled datacenters?

- A foreign-domiciled company is subject to foreign laws, gag orders, and other pressures to cooperate with their intelligence agencies.[5][12][13][34]
- Infiltrators (protected from exposure by the domiciled government using pressure and gag orders) can facilitate secret bulk access to company datacenter information. It is a severe crime expose an undercover government agent.
- Geographically distributed datacenters require on-site auditors in numerous locations
- Replicated information means vulnerabilities could be at any datacenter
- Enormous traffic in and out (including legitimate traffic with other datacenters that might end up with intelligence agencies) makes detecting mass surveillance extremely difficult
- Hardware has continual upgrades and downgrades.
- Software is constantly changing in real-time.

The FBI mandatory backdoor proposal has increased mistrust by foreign governments and citizens alike, with the consequence 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.[3][4][21][35][37] Likewise, every government can require that IoT sold in their country do not have backdoors accessible to other governments.[3][4][23][35][37][39]

On March 2, 2015, President Obama complained about government attempts 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*

Surveillance in foreign-domiciled datacenters

Because no foreign-domiciled company can provide credible assurance that a foreign intelligence agency does not have bulk access to the company's (foreign and domestic) datacenters, the Chinese government is insisting on the following:[5][33]

- "Guarantee the security of user information. To employ effective measures to guarantee that any user information that is collected or processed isn't illegally altered, leaked, or used; to not transfer, store or process any sensitive user information collected within the China market outside China's borders without express permission of the user or approval from relevant authorities."
- "Accept [Chinese government] assessment and verification that products are secure and controllable and that user information is protected etc. to prove actual compliance with these commitments."

Also the newly passed "Anti-terrorism Law" provides that organizations in China will have to "offer technological assistance and cooperation with security departments to help prevent and investigate terrorist activities." In practical terms, that may mean cracking the encryption in an app or device when requested by Chinese security agencies.

firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government."

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.[2][3][4][35]

For national security reasons, many nations could demand that the sensitive information of their citizens not be accessible in the datacenters of foreign-domiciled corporations.[3][4][37][39]

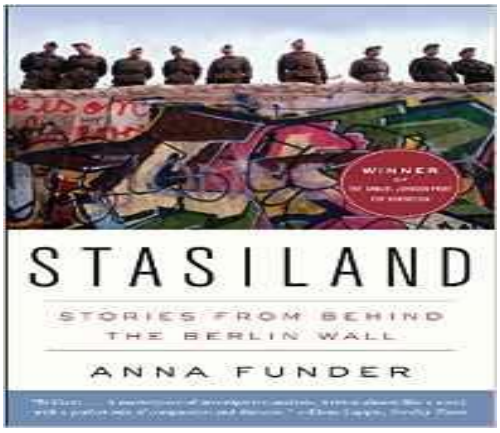
Much greater security can be achieved using imported audited IoT devices than can be achieved using datacenters of a foreign domiciled corporation, which might be operating under a gag order issued by foreign security agencies and known to just a few employees of the corporation with very high-level security clearances.[35][36][37][39][40] Growing mistrust of the security of sensitive citizen information stored in datacenters of foreign-domiciled corporations is a severe problem for multi-nationals.[3][4][23][30]][32][36][39][40] For national security reasons, many nations could demand that the sensitive information of their citizens not be accessible in the datacenters of foreign-domiciled corporations.[3][4][36]

Economic losses of Internet companies due to surveillance in foreign-domiciled datacenters

Other countries are considering adopting policies similar to China, which could cause huge losses to a US domiciled company because it could not export IoT devices (just about everything manufactured) that communicate citizens' sensitive information with the company's datacenters.[10][39] For example, the Advocate General of the European Court of Justice stated: [3]

- "*The access of the United States intelligence services to the data transferred* [to US domiciled companies] *covers, in a comprehensive manner, all persons using electronic communications services, without any requirement that the persons concerned represent a threat to national security.*"
- "*Such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by articles seven and eight of the charter [of fundamental rights of the EU].*"

Mass surveillance by the US Government has been extraordinarily successful with the result that "*Al Qaeda Has Been Decimated*" according to President Obama. Chinese security agencies have accessed US computer systems to collect sensitive information on millions of Americans.[21] Under the likes of the US National Recognizance Organization slogan "*Nothing is beyond our reach*", US security agencies have likewise have conducted extensive surveillance including secretly accessing and taking control of information systems in China.[3][4][32] The extreme effectiveness of electronic mass surveillance has demonstrated how risky government surveillance (including secretly accessing and taking control of information 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 COINTELPRO), Joe McCarthy (US Senate Permanent Subcommittee on Investigations), Erich Mielke (Stasi)[9], *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.*"

Mike Rogers (current Director of NSA) on at the Aspen Security Conference on July 23, 2015 said, "*That the capabilities of the* [US] *government will not be used against us* [US citizens] *indiscriminately is fundamental to our structure as a nation*."

Unconstitutional Surveillance by US Presidents

- 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.

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.)

As each cyberattack increases pressure to react, security agencies in many countries can obtain bulk access to more and more information in datacenters using interconnectivity with government surveillance datacenters in order to speed and coordinate government security efforts.[10][36][40] The exact nature of interconnectivity with government security datacenters is in each case a closely guarded corporate secret that can be enforced by government gag orders.[10][36][40]

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.[4][36][40] Edward Snowden at IETF 93 characterized the path from CyberLocalism to CyberTotalism as follows: "*idea of a simple core and smart edges -- that's what we planned for. That's what we wanted. That's what we expected, but what happened in secret, over a very long period of time was changed to a very dumb edge and a deadly core*."

IoT Security Commission (ISC)

- jurisdiction over all providers of IoT equipment in the US:[16]
- require that every kind of IoT device be audited, *e.g.*, using operational bi-simulation against a publicly available operational specification overview.
- require that corporate security reports 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.
- 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
- enforce compliance with specific legal mandates, *e.g.*, the use of RAM-processor encryption and every-word-tagged extensions of ARM and X86 processors.

To facilitate faster and more comprehensive security operations, security agencies need to use corporate information mining tools in corporate datacenters for (perhaps with some direct costs reimbursed by the government[25]) thereby making corporate engineers and executives *increasingly complicit in mass surveillance*.[4][18][25][36][40] Furthermore, businesses can be harmed by their inability to change datacenter operations because it would disrupt government surveillance. Government security agencies 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.[3][4][15][25][36] Consequently, corporations need to better understand that sensitive citizen information is not always a corporate asset and instead can be a toxic corporate liability.[3][4][5][8][15][18][25][36]

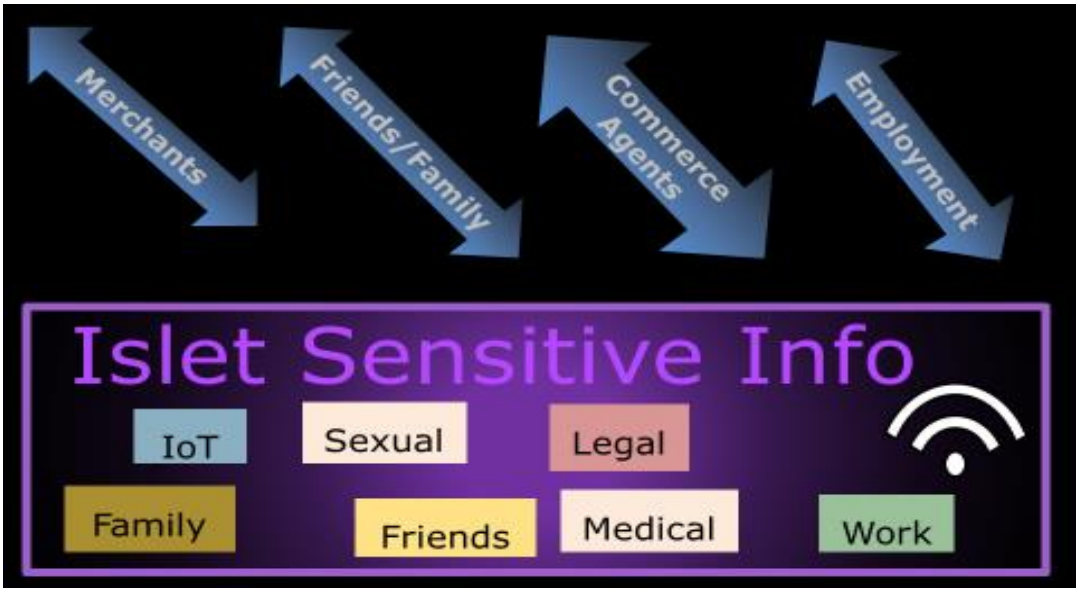
Fortunately, there is an alternative to CyberTotalism: *CyberLocalism* is a system in which a citizen's sensitive information is stored locally in on their own equipment (without backdoors) – *the antithesis of both Datacenterism and CyberTotalism*.[17]

Abuse of sensitive information

What sensitive information was used against the citizen and was it done in secret?

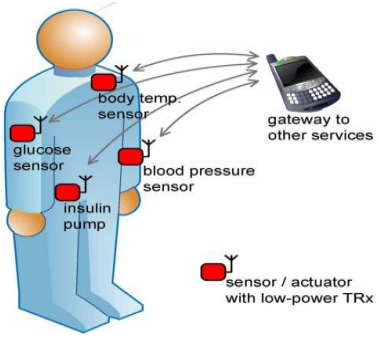
CyberLocalism might never come to fruition unless it is supported by a business model that is more efficient and effective than the currently popular system of Datacenterism.[17] Consequently, the Standard IoT™ international nonprofit standards organization has proposed Islets™ information coordination systems as the foundational basis for information coordination and

interaction services for a citizen's sensitive IoT information. Each Islet can be hosted on a citizen's own equipment, *e.g.*, routers, body-sensor computer networks[26], refrigerators, car, cell phones, TVs, autos, and PCs.



Islet™ Information Coordination and Interaction for Sensitive Info

An Islet can provide additional capabilities that are not currently available for coordinating and interacting with cyberthings[v] 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.*) [17]



Body-Sensor Computer Networks[26]

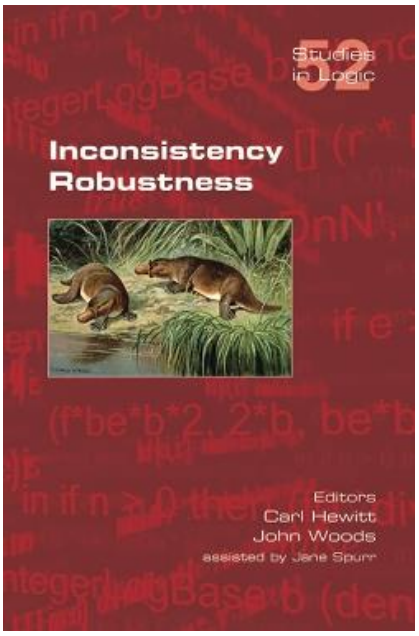
Of course, all of the convenience that is currently available must also be available so that an Islet can access the Internet to provide scalable search, retrieval, and collaboration using commercial datacenters in cooperation with other citizens' equipment.

An Islet can run on multiple citizen devices (*e.g.*, phones, refrigerators, insulin pumps, bedroom TVs, brain implants, home routers, *etc*. These devices are connected only intermittently and some of them may fail permanently. Consequently an Islet must deal with asynchronously-arriving information

[v] A *CyberThing* is a physical or electronic artifact of Internet systems, e.g., body-sensor computer networks, light fixture, email, refrigerator, voice mail, cellphone, SMS, and electronic door locks. on the Internet.

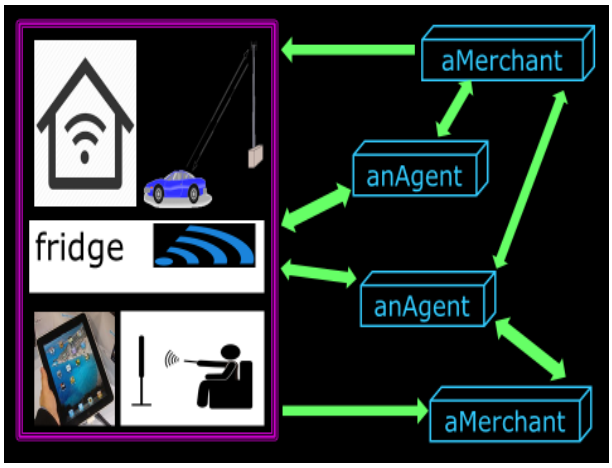
from various devices and from the outside Internet. Fortunately, Actors[16] provide a suitable foundation for modeling and implementing Islets.

Classical logic (a foundation for relational databases) and probability theory do *not* provide a suitable foundation for IoT 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).[16]



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).

Recent advances in the development of inconsistency-robust information systems technology[16] can be used to facilitate new business implementations that are more *effective*, *pervasive*, and *profitable* by improving interactions among consumers and merchants 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.



Islet Coordinating with Agents and Merchants Business Model

Attempting to provide CyberThing coordination and interaction services for a

citizen by patching together datacenter services from fierce competitors[vi] is much more difficult than using an Islet.[17]

Sensitive information is nonpublic information whose revelation can potentially harm a citizen, *e.g.*, medical (including psychiatric), legal, financial, sexual, political, and religious. 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.[15]

CyberLocalism requires greater security of citizens' IoT devices because currently state-sponsored intruders can secretly access and take control of almost any citizen's personal cellphone[10][32], computer, body-sensor computer network[26], *etc.* on the Internet.

Increase IoT Security

- Public keys for device ownership
- Authenticated public keys for citizens
- Bio-authentication
- Hardware protection of software Actors (applications as well as their Java and C/C++ objects)
  - RAM-processor package encryption
  - Every-word-tagged architecture

Islets advantages over datacenterism:[10][23][33]

- lower communications cost because it is not necessary to always communicate with datacenters
- faster response because local operations can be faster than always interacting with potentially overloaded datacenters,
- better coordination of IoT because it can be difficult to get datacenters of *fierce* competitors to coordinate concerning the interoperation of a citizen's IoT devices,
- greater reliability because communication with datacenters might be interrupted[[24]
- better protection of a citizen's sensitive information because it is not always available in datacenters accessible by security agencies.
- improved coordination with merchants
  - more relevant and less intrusive advertising
  - better coordination between merchants

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 as well as 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.)

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

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 as well as 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.[16][17]

The Internet of Things (IoT) has the potential to greatly improve human health. Large-scale behavioral change can be facilitated by improved human interaction and awareness. Also, treatment, therapy, and physical movement can be guided and assisted.

Hardware security for IoT

- 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.
- Every-word-tagged extensions of ARM and X86 processors are 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, and mail systems) will need to be upgraded to use tags.
- On a processor package, encryption can be used to augment error correction on bus communication between hardware Actors in order facilitate auditing of the processor.

However, IoT also poses extreme challenges for medical ethics. Commercial health and medical IoT development has been problematic. Enormous amounts of sensitive medical information are being stored in datacenters of intense competitors. Much of the most extremely sensitive information is being sold by data brokers. Consumer health and medical IoT are becoming ever more intimate. Many people have pacemakers and even more have insulin pumps. Soon there will be anti-fall IoT for the elderly. DARPA is developing an implantable neural interface able to provide unprecedented signal resolution and data-transfer bandwidth between the human brain and the digital world. Before long, many workers and soldiers may not be competitive unless they have brain implants..[6][7][29]

Proposals for IoT mandatory backdoors are especially problematic. The UK Parliament is set to pass legislation (the "Investigatory Powers Bill"[28]) that no IoT information will be immune to police surveillance and control. The FBI is making similar demands for

backdoors. Prominent US legislators have vowed that the issue will soon be taken up by Congress.

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. The speed of cessation will depend in large in part on how fast the security measures presented in this article are deployed.[16]

The presumption is that intelligence agencies have access to all information in datacenters of foreign-domiciled companies. Consequently, a nation's security requires that its citizens' sensitive information not be accessible in datacenters of foreign-domiciled companies. Furthermore, every imported IoT device (cell phone, refrigerator, car, insulin pump, TV, climate-control system, etc.) is going to have to be certified not to have a backdoor available to a foreign intelligence agency. Thus US industry faces the crises that its current IoT business model is about to become illegal. Already experts put loses to US tech industry as a whole, not just the cloud computing sector, north of $180B and still climbing.[5][16] Since almost all manufactured exports will soon include IoT, we can expect that losses to US industry will be well north of $3T unless drastic changes are made.

Advertising Competitive Race

In a competitive race down an ethical abyss, many Internet companies depend on ever greater surveillance in order to better target consumers for advertising.[9][18][20] *However, a nation's security depends on limiting surveillance of their citizens by foreign security agencies enabled by Internet companies domiciled in other nations*.[8][10][23]

Going forward, security agencies have proposed mandatory backdoors for all IoT in order that they can always be able to surveil anything and everything that might be deemed necessary by the government.[17] As indicated by NSA Director Mike Rogers, mandatory backdoors mean that security agencies of each country surveil citizens in their own country[17] and can swap surveillance information with other countries. IoT Mandatory backdoors are fraught with peril because making it possible for security agencies to secretly access and take control of each individual IoT device can make it very difficult to prevent security agencies from accessing and controlling large numbers of devices thereby abusing their surveillance capabilities.[16] A critical security issue is that after a backdoor has been exercised to take control of a citizen's IoT device without their awareness, the device thereby becomes somewhat *less* secure because of potential vulnerabilities in the new virtualized system used

to take control of the device.[0][1][10]][11][17][32] Of course, any attempt to *change* the device's application behavior can introduce additional vulnerabilities.

Arguments Against IoT Mandatory Backdoors

- Economic
  - diminish size of IoT market
  - hamper IoT exports and imports
- National defense
  - auditing IoT against backdoors of foreign intelligence agencies becomes more difficult
- Loss of civil liberties due to mass surveillance
- Breakdown of Societal Trust
  - Stasiland turbo-charged
- Against medical ethics

The right against self-incrimination by body-sensor computer networks[26] will be become increasingly important. Consequently, IoT mandatory backdoors could become a severe threat to citizens' rights. Just the public awareness itself that any IoT device (*e.g.* cell phone[11][32], TV, auto, PC, body-sensor computer networks[26]) could be secretly accessed and controlled by security agencies could be extremely corrosive to social arrangements.[3][4][11][27] Going forward, IoT 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.[17] It was extremely abusive to use people's sensitive information against them as was done by the Stasi, Hoover's FBI COINTELPRO, *etc*.[9][15] Because of improving information technology using IoT (*e.g.* cell phone[11][32], TV, auto, PC, body-sensor computer networks[26]), preventing such abuses will become ever more important.[3][4][5][18][20] Adopting Islets would go a long way toward protecting citizens' sensitive information against both government and corporate abuse.[17]

Eventual fate: transnational datacenters with sensitive citizen info

1. **Datacenter Info Localization**: Citizens' datacenter information must be stored domestically so that can law enforcement can have quick access without foreign hindrance
2. **Corporate Balkanization**: Corporations that store sensitive citizen information in their datacenters must be domestically incorporated to ensure that foreign intelligence agencies do not have bulk access to the information.

Mandatory secret surveillance by each nation's security agencies imposed on corporations domiciled in the nation could tremendously reduce the power and resources of multinational Internet companies[vii] 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 agencies of other countries.[5][23][25][30]][32][36] One outcome is that multi-nationals to become separate corporations domiciled in each nation (for security reasons) to serve just

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

that nation, which is already happening in China and other countries.[3][4][5] A multinational could take the proceeds of the IPO for spinning off a separate company in each country as a franchise. Attestation and RAM-processor package encryption technology will make corporations domiciled in each country more affordable by enabling them to more securely share capacity in datacenters located in each country.[16]

On August 1, 2007, (then Senator) Barack Obama called for an alternative to oppressive mass surveillance saying "That means no more illegal wiretapping of American citizens. ... No more tracking of citizens who do no more than protest a misguided war."

Sleepwalking into Cybertotalism

- If we do nothing, we sort of sleepwalk into a total surveillance state where we have both a super-state that has unlimited capacity to apply force with an unlimited ability to know (about the people it is targeting)–and that's a very dangerous combination.
- That's the dark future. The fact that they know everything about us and we know nothing about them – because they are secret, they are privileged, and they are a separate class… the elite class, the political class, the resource class – we don't know where they live, we don't know what they do, we don't know who their friends are. They have the ability to know all that about us.
- This is the direction of the future, but I think there are changing possibilities in this."[31]

Edward Snowden

Distributed Encrypted Public Recording (DEPR) inhibits mass surveillance by requiring a court warrant to access encrypted information recorded by distributed parties (*e.g.*, stores, restaurants, sports events, parks, theaters, *etc*.) with a write-once log kept for all accesses thereby making mass surveillance more costly, both politically and economically. Advanced Inconsistency Robust[16] information technology can be a very powerful tool for catching and prosecuting criminals using DEPR because it can provide principled methods and technology for processing large amounts of pervasively inconsistent information.[16]

The government use of the All Writs Act (which predates the Bill of Rights) in the Apple case is a Trojan Horse that threatens loss of our civil liberties. The use is an extreme usurpation of power that is not allowed by the Constitution. In fact, Congressional intent in legalizing the use of unbreakable encryption in CALEA was follows:

> "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, [this bill] protects the right to use encryption."

Right against self-incrimination

- Citizens' IoT devices should not require that they surrender control of the devices, or sensitive data, to anyone except those who have a duty of care for them and have their informed consent.
- This means that citizens' information on these devices should not be taken and used against their interests, directly or indirectly.

Using All Writs to give the government power to order companies to redesign their products to government specifications (US.gov OS?) will result in endless work for which the government is both unqualified and ill-equipped. According to Apple, the All Writs Act

> "does not give the district court a roving commission to conscript and commandeer Apple in this manner ... In fact, no court has ever authorized what the government now seeks, no law supports such unlimited and sweeping use of the judicial process, and the Constitution forbids it...
>
> Indeed, examples abound of society opting not to pay the price for increased and more efficient enforcement of criminal laws. For example, society does not tolerate violations of the Fifth Amendment privilege against self-incrimination, even though more criminals would be convicted if the government could compel their confessions. Nor does society tolerate violations of the Fourth Amendment, even though the government could more easily obtain critical evidence if given free rein to conduct warrantless searches and seizures... The government's desire to leave no stone unturned, however well intentioned, does not authorize it to cut off debate and impose its views on society."[1]

For example, the current government order will not work for the next generation of iPhones. Should government have the power to order Apple to redesign their next generation so that Apple could comply with the current order that Apple is appealing? Can the government prohibit the importation of Samsung phones for which Samsung has no ability to break in and read encrypted information?

Suppose that a newspaper has published a story about fixing football games that has resulted in the indictment of a quarterback and betting ring. However, the prosecutor fears that they lack sufficient evidence to convict. The reporter who wrote story is then arrested on a DUI charge and his iPhone is seized. The prosecutor suspects that the iPhone has messages that could aid the prosecution. Should government have the power to order Apple to write new software to give the government the ability to decrypt information on the iPhone (which is technically called creating a "backdoor")?

The Internet of Things (IoT) is becoming pervasive in all aspects of life including personal, corporate, government, and social. Security agencies have proposed that it must be possible for them to secretly access and take control of any individual IoT device if they have been authorized. However adopting their proposal would make it very difficult to prevent them from accessing and controlling large numbers of devices and abusing their surveillance capabilities.

Congress should correct the usurpation of power that would result from the use of All Writs to require creation of mandatory backdoors. Even before the Apple case, Congressman Ted Lieu introduced legislation to disallow state governments to mandate the ability to defeat device security. Lieu's proposed legislation should be strengthened as follows to apply to the entire US government:

> The US government or any of its political subdivisions including a State or political subdivision of a State may not order or coerce that a manufacturer, seller, developer, or provider of any computer hardware, computer software, or electronic device that is made available to the general public:
>
> 1. Design, alter or modify the security features in its product in an effort to allow any federal agency or instrumentality of a State, a political subdivision of a State, or, of course, the United States to obtain information in the product.
> 2. Have the ability to decrypt or otherwise provide intelligible information that is encrypted or otherwise rendered unintelligible using its product.

The above proposed legislation strikes a proper balance between protecting our civil liberties and the need to catch and prosecute criminals: On one hand, it protects the 5th Amendment Right against self-incrimination by prohibiting mandatory IoT backdoors. On the other hand, it allows all activities outside the homestead to be subpoenaed using Distributed Encrypted Public Recording

Maintaining civil liberties

Mandate that all IoT devices (cell phones, climate control systems, televisions, brain implants, cars, refrigerators, insulin pumps, *etc*.) must be certified (audited) against backdoors.

Available alternatives are summarized in the following table:

Enterprise, Military, and Citizen Islets™ Information Coordination[17]	**Datacenterism**[5][8][10][13][17][23][25][28][30]][34][36][39][41]
Business model[9][17] Islet-agent-merchant brokering[10]	**Business model**[9][16][41] Ever increasing consumer surveillance for better targeted advertising
Security model[9][10][17] ○ RAM-processor package encryption to protect applications from memory-bus devices (USB, disk, baseband processors, etc.), other applications, and also from hypervisors and operating systems ○ Every-word tagged architecture to protector Actors from other Actors in the same process ○ Strong biometric authentication ○ Auditable public keys for citizens and IoT ownership ○ *No mandatory backdoors in citizens' Islets*	**Security model**[10][17][28][39][41] Security agencies have access to all information of companies domestically domiciled (with gag orders) including datacenters located in foreign countries
Surveillance **Distributed Encrypted Public Recording (DEPR)**[17] • Ability to subpoena all activities outside the homestead • Accessible only by individualized court warrant • Totally inaccessible after a set time period (enforced by encryption)	**Surveillance** **IoT Mandatory backdoors**[5][11][17][28][39] • Surveil thoughts including brain implants • Any IoT device can be accesses and controlled if connected to the Internet • Includes body-sensor computer networks • Each nation surveils its own citizens • Potential security vulnerabilities after security services have taken control of a device

Available alternatives

Acknowledgements
This article has greatly benefited from detailed critiques and organizational suggestions of Alan Karp and Andy Rosenbloom, editorial suggestions of Dennis Allison, Henri Gouraud and Richard Waldinger, comments by Chip Morningstar,

conversations with Dan Boneh, Whit Diffie, Dan Flickinger, Erik Meijer, Mark Musen, John Perry, Jeff Rulifson, Ken Taylor, George Triantis, and Mary-Anne Williams, and suggestions of Ron Rivest and Peter Neumann. John Dalton provided design and editorial consulting.

The author's Erlang keynote address *Actors for CyberThings*[17] covers some of the material in this article.

The Author

Professor Carl Hewitt is the creator (together with his students and other colleagues) of the Actor Model of computation, which influenced the development of the Scheme programming language and the π calculus, and inspired several other systems and programming languages. The Actor Model is in widespread industrial use including eBay, Microsoft, and Twitter. For his doctoral thesis, he designed Planner, the first programming language based on pattern-invoked procedural plans.

Professor Hewitt's recent research centers on the area of *Inconsistency Robustness*, *i.e.*, system performance in the face of continual, pervasive inconsistencies (a shift from the previously dominant paradigms of inconsistency denial and inconsistency elimination, *i.e.*, to sweep inconsistencies under the rug). ActorScript and the Actor Model on which it is based can play an important role in the implementation of more inconsistency-robust information systems.

Hewitt is Board Chair of iRobust™, an international scientific society for the promotion of the field of Inconsistency Robustness. He is also Board Chair of Standard IoT™, an international standards organization for the Internet of Things, which is using the Actor Model to unify and generalize emerging standards for IoT. He has been a Visiting Professor at Stanford University and Keio University and is Emeritus in the EECS department at MIT.

References

[0] Harold Abelson, Ross Anderson, Steven Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter Neumann, Susan Landau, Ronald Rivest, Jeffrey Schiller, Bruce Schneier, Michael Specter, Daniel Weitzner. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* MIT-CSAIL-TR-2015-026. July 6, 2015.

[1] Apple, Inc. "Apple Inc.'s Motion to Vacate Order Compelling Apple Inc.to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance" February 25, 2016.

[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] Yves Bot. *Opinion of Advocate General to European Court of Justice.* Case C-362/14 "Maximillian Schrems versus Data Protection Commissioner" September 23, 2015.

[4] 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.

[5] China. *Information Technology Product Supplier Declaration of Commitment to Protect User Security* Pledge circulated by Chinese government to companies that desire to do future business in China. 2015.

[6] Emma Cott. *Prosthetic Limbs, Controlled by Thought.* New York Times. May 20, 2015.

[7] DARPA. *Bridging the Bio-Electronic Divide: New effort aims for fully implantable devices able to connect with up to one million neurons.* DARPA. January 19, 2016.

[8] Disconnect, Inc. *Complaint of Disconnect, Inc.* European Antitrust Commission. Case COMP/40099. June 2015.

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

[10] Rian Gallagher. *Revealed: How DOJ Gagged Google over Surveillance of WikiLeaks Volunteer*. The Intercept. June 20, 2015.
[11] Ryan Gallagher and Glenn Greenwald. *How the NSA plans to infect 'millions' of computers with malware. The Intercept.* March 12, 2014.
[12] John Gilmore and Mike Wiser. *Secrets, Politics and Torture*. PBS Frontline. May 19, 2015.
[13] Jennifer Granick. *OmniCISA Pits DHS Against the FCC and FTC on User Privacy.* Just Security Blog. December 15, 2015.
[14] Shane Harris. *@War: The Rise of the Military-Internet Complex.* Eamon Dolan/Houghton Mifflin Harcourt. Boston, MA, 2014.
[15] Florian Henckel von Donnersmarck. *The Lives of Others*. Wiedemann & Berg, et. al. 2006.
[16] Carl Hewitt and John Woods assisted by Jane Spurr, Editors. *Inconsistency Robustness*. College Publications. 2015.
[17] Carl Hewitt. *Actors for CyberThings.* Erlang Keynote. YouTube. March 23, 2015.
[18] Cullen Hobak. *Terms and Conditions May Apply.* Phase 4 Films. 2013.
[19] Justin Jouvenal. *The new way police are surveilling you: Calculating your threat 'score'*. Washington Post. January 10, 2016.
[20] Steve Kroft. *The Data Brokers: Selling your personal information.* 60 Minutes. March 9, 2014.
[21] Edward Lee. *Swarm Boxes*. SwarmLab UC Berkeley. March 19, 2015.
[22] Ted Lieu. *Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016*.
[23] Jenna McLaughlin *Edward Snowden Explains Why Apple Should Continue To Fight the Government on Encryption*. The Intercept. July 31, 2015.
[24] Ellen Nakashima. *With a series of major hacks, China builds a database on Americans.* Washington Post. June 5, 2015.
[25] Ewen MacAskill. *NSA paid millions to cover Prism compliance costs for tech companies.* The Guardian. August 23, 2013.
[26] Jens Masuch and Manuel Delgado-Restituto. *Ultra Low Power Transceiver for Wireless Body Area Networks.* Springer. 2013.
[27] Bill Marczak, *et. al.. China's Great Cannon*. University of Toronto. April 10, 2015.
[28] Theresa May (UK Home Secretary). *Draft Investigatory Powers Bill.* Presented to Parliament. November 2015.
[29] Abby Philip. *A paralyzed woman flew an F-35 fighter jet in a simulator — using only her mind.* Washington Post. March 3, 2015..
[30]] Salvador Rodriguez. *NSA 'Equation' Fallout: Experts Say Damage To US Tech Firms Could Top $180B* International Business Times, February 15, 2015.
[31] Arundhati Roy. *Edward Snowden meets Arundhati Roy and John Cusack: 'He was small and lithe, like a house cat'* The Guardian. November 28, 2015.
[32] Jeremy Scahill and Josh Begley. *The CIA Campaign to Steal Apple's Secrets*. The Intercept. March 10, 2015.
[33] Eric Schlosser. *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*. Penguin Books. 2014.
[34] Scott Shane and Colin Moynihan. *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s* NY Times. September 1, 2013.
[35] Dave That, Vint Cerf, et. al. *Request for the Allowance of Optional Electronic Labeling for Wireless Devices* Letter to US FCC. RM11673. 2015.
[36] Sam Thielman. *Cybersecurity bill could 'sweep away' internet users' privacy, agency warns.* The Guardian. August 3, 2015.
[37] Daniel Thomas. *Huawei does not pose risk to UK national security, report finds.* Financial Times. March 31, 2015.
[38] US National Security Council. *Draft paper on technical options for the encryption debate.* leaked 2015.
[39] Cyrus R. Vance, Jr. Written Testimony Before the United States House of Representatives Committee on the Judiciary. March 1, 2016.
[40] Ariane Wu. *The Secret History of American Surveillance.* Reveal News. October 15, 2015.
[41] Shoshana Zuboff. *Big other: surveillance capitalism and the prospects of an information civilization.* Journal of Information Technology Vol. 30. 2015.