Security without Mandatory Backdoors

Carl Hewitt

▶ **To cite this version:**

Carl Hewitt. Security without Mandatory Backdoors. 2015. hal-01152495v6

HAL Id: hal-01152495

https://hal.science/hal-01152495v6

Preprint submitted on 9 Sep 2015 (v6), 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

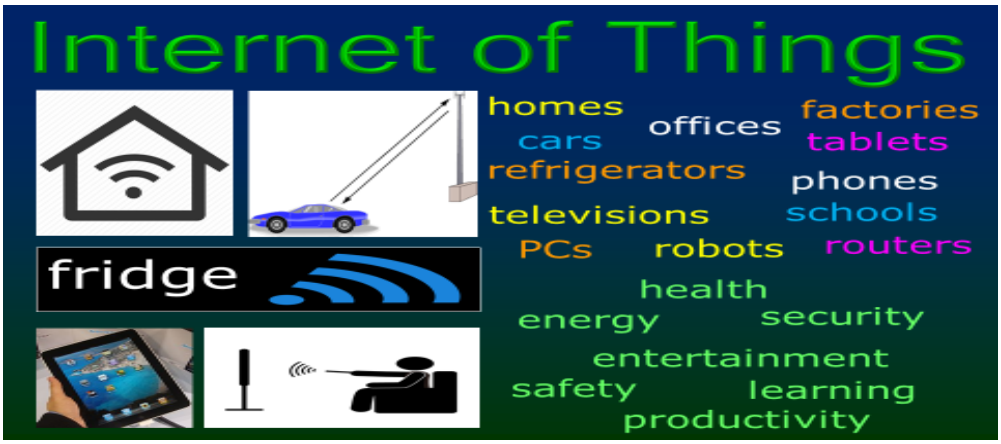
Security without Mandatory Backdoors

Using Distributed Encrypted Public Recording to Catch Criminals

Our greatest enemy is our own apathy.
Bill Mullinax

Carl Hewitt

The Internet of Things (IoT)[i] is becoming pervasive in all aspects of life including personal, corporate, government, and social. Adopting mandatory backdoors[ii] for every IoT device ultimately means that security agencies of each country surveil IoT in their own country and perhaps swap surveillance information with other countries.[8][22][23] 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.[6][7][8][22][23] Also, adopting mandatory backdoors would be corrosive to civil liberties because any phone, body-sensor computer network[20], TV, and other IoT device[iii] could be secretly accessed and controlled without any awareness by those present using the device.[6][8][11][23][24]26] A critical security issue is that after a mandatory 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.[1][7]][8][15][23]



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 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 distributed[iv] public and private organizations keep encrypted electronic records of all activity that takes place in public places including tracking automobiles, cell phones locations, humans (using facial recognition), and all financial transactions. The records can be decrypted only by court subpoena using both a key kept by the recording establishment and a key provided by the court. If not subpoenaed 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[12] information technology can be a very powerful tool for catching criminals using DEPR. Using DEPR is a less risky to citizen security than requiring mandatory backdoors for all IoT devices.

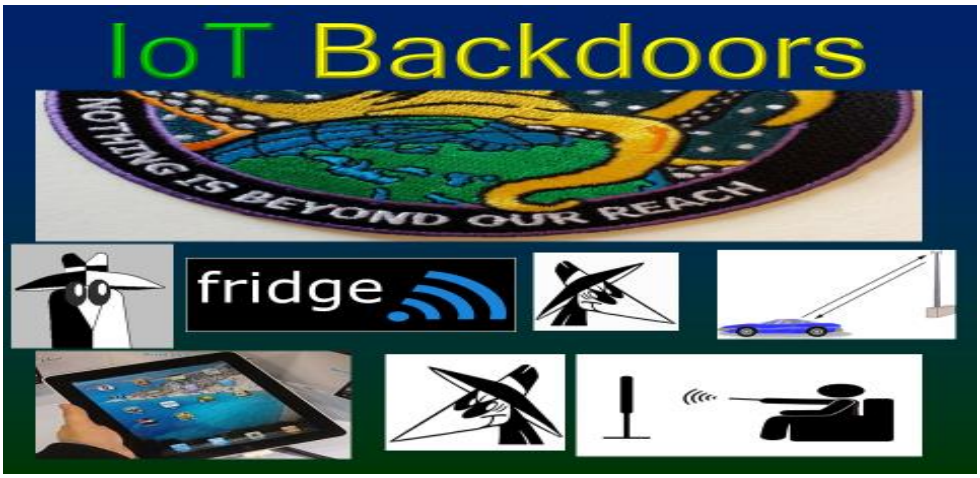
However, IoT devices will require much more powerful integrated security technology than the current patchwork, which can almost always be circumvented by state-sponsored intruders.[4][5][8][12][18][21][23][24] Using mechanisms outlined in this article, the US can immediately launch a crash program to secure IoT devices (including corporate, citizen, utility, and government) thereby making them dramatically more secure.[15]

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 governmen*t."

There are huge security advantages for the US and EU taking a leadership position in adopting auditing against mandatory backdoors for IoT devices since the rest of the world could well follow their lead..[12]

However, the Obama administration made no similar complaint about FBI Director James Comey's proposal on October 17, 2014 that CALEA be expanded so that every cell phone, body-sensor computer network[20], 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[8][23] with the assent of US courts.

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



Power of 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. These arrangements would have huge consequences for Internet interconnectivity, international trade of IoT products and the competitiveness of US manufacturers in general.[2][8][17][22][23][26]

Mandatory backdoor technology can build on already developed CIA/GCHQ/NSA surveillance technology including QUANTUM, SMURF, TURBINE, TURMOIL, UNITEDRAKE, WARRIOR PRIDE, VALIDATOR, *etc*.[8][23] The equivalent of a different public key can be installed by the manufacturer on each device. For each public key, a private key can be split and sent to government authorities of the nation in which the device is to be sold. 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.[1][25] 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

> Adopting mandatory backdoors for every IoT device ultimately means that security agencies of each country surveil IoT in their own country and perhaps swap surveillance information with other countries.[8][21] Also, adopting the mandatory backdoor proposal would make it very difficult to prevent security services from accessing and controlling large numbers of devices and abusing their surveillance capabilities.[6][7][8][21][22] In addition, adopting mandatory backdoors would be corrosive to 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.[6][8][11][22][25] Furthermore, after a security service has secretly taken control of an IoT device, the device thereby becomes *less* secure against other potential attackers.[1][7][22]

small number of inside conspirators by using multiple command centers with split keys. A critical security issue is that after a mandatory 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.[8][15][23]

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.[2][27] 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[10] and kinetic responses to cyberattacks because of potential vulnerabilities in the many different government backdoor implementations.[21] Also, mandatory backdoors can increase the security risks to military equipment because they might be exploited by enemy forces. Furthermore, mandatory backdoors can enormously increase the power of government security agencies.[6][23][24][26]

> According to then Vice Chairman of the Joint Chiefs of Staff Admiral James Winnefeld on May 14, 2015, "*But I think we would all win if our* [Internet] *networks* [IoT] *are more secure. And I think I would rather live on the side of secure networks* [of IoT] *and a harder problem for Mike* [NSA Director Mike Rogers] *on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it's not only is the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber*." [26]

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][7][12][19][22][26] 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.[4][22] "*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*.

The NSA/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.[2][16][27] Likewise, every government can require that IoT sold in their country do not have backdoors accessible to other governments.[2][17][27]

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] An IoT Security Commission (ISC) could to be established with jurisdiction over all providers of IoT equipment in the US: [12]

> 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 extensions of ARM and X86 processors.

No means are known by which to securely audit operations of a corporation's geographically distributed datacenters against access/control by security agencies in which the corporation is domiciled. One difficulty is that datacenters exchange enormous amounts of diverse kinds of information with each as well as with government/other corporate datacenters. Another difficulty is that each datacenter's equipment and diverse software is continually being updated. Auditing of a corporation's geographically distributed datacenters would require an onsite team at each datacenter to audit ongoing operations and continual hardware/software changes. Gag orders (known to just a few employees of the corporation with very high-level security clearances) can be imposed that security agencies access/control not be revealed even for datacenters that are physically located in countries other than the one where the corporation is domiciled.[4][7][8][19][22] Consequently, it is extraordinarily difficult to audit against government security agencies access/control in a corporation's geographically distributed datacenters known to just a few employees of the corporation with very high-level security clearances.[4][7][19][22] Growing mistrust of the security of sensitive citizen information stored in datacenters of foreign-domiciled corporations is a severe problem for multi-nationals.[2][4][9][22] 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.[2]

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.[24][27] Growing mistrust of the security of sensitive citizen information stored in datacenters of foreign-domiciled corporations is a severe problem for multi-nationals.[2][17][22][23][26] 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.[2]

Mass surveillance by the US Government (in Afghanistan, Pakistan, Somalia, Yemen, *etc*.) 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.[18] 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.[2][4][23] The extreme effectiveness of electronic mass surveillance (in Afghanistan, *etc*.) 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), Joe McCarthy (US Senate Permanent Subcommittee on Investigations), Erich Mielke (Stasi)[6], *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*."

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. 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.[7]

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.[2][24] 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*."

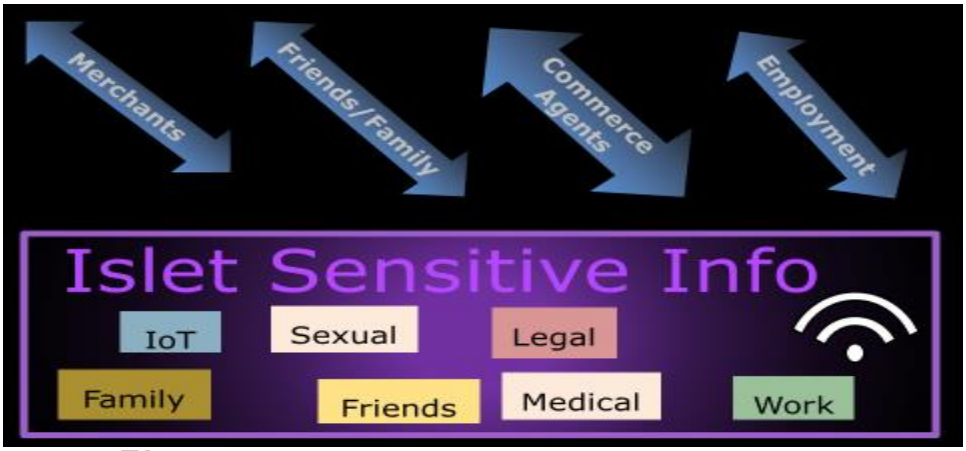
To facilitate faster and more comprehensive security operations, security agencies need to use corporate information mining tools in corporate datacenters for (perhaps with some direct costs reimbursed by the government[19]) thereby making corporate engineers and executives *increasingly complicit in mass surveillance*.[19] 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.[15][19] Consequently, corporations need to better understand that sensitive citizen information is not always a corporate asset and instead can be a toxic corporate liability.[2][5][15][19]

In a competitive race, many Internet companies depend on ever greater surveillance in order to better target consumers[5] for advertising. However, a nation's security depends on limiting surveillance of their citizens by foreign security agencies enabled by Internet companies domiciled in other nations.[7][22]

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*.[15]

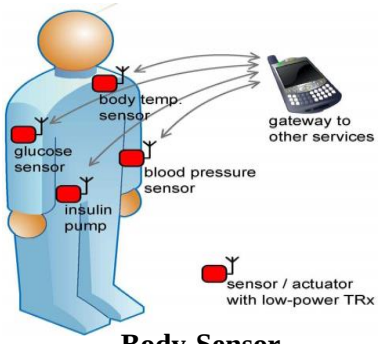
CyberLocalism might never come to fruition unless it is supported by a business model that is more efficient and effective than the currently popular system of Datacenterism.[15] Consequently, the Standard IoT™ international nonprofit standards organization has proposed Islets™ information integration 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[20], refrigerators, cell phones, TVs, autos, PCs, *etc.*

- *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.*



Islet™ Information Coordination and Interaction for Sensitive Info

The right against self-incrimination by body-sensor computer networks[20] will be become increasingly important thereby making mandatory IoT backdoors a severe threat to citizens' rights.



Body-Sensor Computer Networks[20]

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.*)[3], *Social* (schedule, friends, family, *etc.*), and *Work* (contacts, schedule, colleagues, *etc.*) [15]

Classical logic (a foundation for relational databases) is *not* 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[vi] information systems technology can be used to more safely

[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, electronic door lock, *etc*. on the Internet.

[vi] *Inconsistency robustness*[12] is information system performance in the face of continual, pervasive inconsistencies.

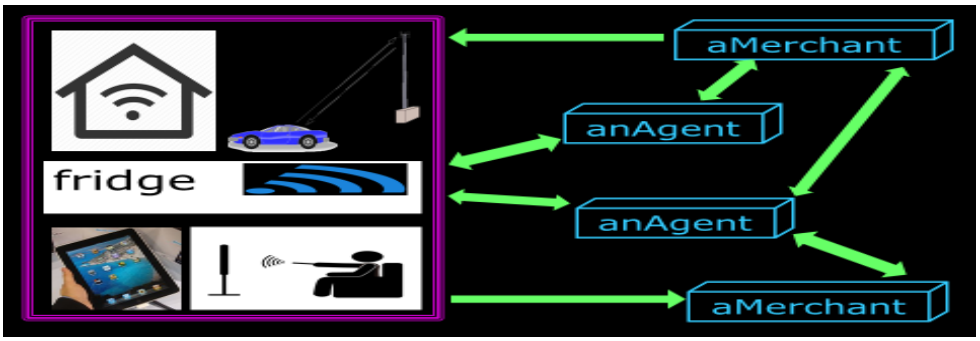
Inconsistency robustness is both an observed phenomenon and a desired feature.

reason about pervasively inconsistent information (even without knowing which pieces of information might be inconsistent).[12]

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).

Cyberlocalism has important advantages over datacenterism: [7] [15]

- 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[[16]
- better protection of a citizen's sensitive information because it is not always available in datacenters accessible by security agencies.



Islet Coordinating with Agents and Merchants Business Model

Recent advances in the development of inconsistency-robust information systems technology[13] 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.

Attempting to provide CyberThing coordination and interaction services for a citizen by patching together datacenter services from fierce competitors[vii] is much more difficult than using an Islet.[15]

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.[11]

The US Senate Select Committee *Final Report on Intelligence Activities and the Rights of Americans* [1976] documented Constitutionally illegal surveillance by *all* modern Presidents [summarized in Wikipedia]:

- 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.

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

CyberLocalism requires greater security of citizens' Internet of Things devices because currently state-sponsored intruders can secretly access and take control of almost any citizen's personal cellphone[8][23], computer, body-sensor computer network[20], *etc.* on the Internet.

To achieve adequate security, CyberLocalism has the following requirements:[14]

- strong personal authentication, *e.g.*, using (3D) continuous interactive bio-authentication instead of passwords.
- strong, ubiquitous public key authentication is required 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. A citizen or organization can have more than one authenticated public key 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 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.

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.
- 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, mail systems, *etc.*) 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.

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.[14]

Because of impending endpoint security improvements described in this article, it can become extremely difficult even for state-sponsored intruders to secretly access and take control of IoT devices, e.g., body-sensor computer networks[20], cell phones[8][23], 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. The speed of cessation will depend in large in part on how fast the security measures presented in this article are deployed.[12]

Security agencies have proposed mandatory backdoors for all IoT.[15] As indicated by NSA Director Mike Rogers, mandatory backdoors mean that security agencies of each country surveil citizens in their own country[15] and can swap surveillance information with other countries. Adopting the mandatory backdoor proposal is 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.[12] A critical security issue is that after a mandatory 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.[1][7][8][15][23] Of course, any attempt to *change* the device's user behavior can introduce additional vulnerabilities.

The right against self-incrimination by body-sensor computer networks[20] will be become increasingly important. Consequently, mandatory IoT backdoors could become a severe threat to citizens' rights. Just the public awareness itself that any IoT device (*e.g.* cell phone[8][23], TV, auto, PC, body-sensor computer networks[20]) could be secretly accessed and controlled by security agencies could be extremely corrosive to social arrangements.[2][24] 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.[15][24] It was extremely abusive to use people's sensitive information against them as was done by the Stasi, Hoover's FBI, *etc*.[6][11] Because of improving information technology using IoT (*e.g.* cell phone[8][23], TV, auto, PC, body-sensor computer networks[20]), preventing such abuses will become ever more important.[2][24] Adopting Islets would go a long way toward protecting citizens' sensitive information against both government and corporate abuse.[15]

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[viii] 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.[2][17][19][22][23][26] One outcome is that multi-nationals to become separate corporations domiciled in each nation (for security reasons) to serve just that nation, which is already happening in China and other countries.[2][4] 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.[12]

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 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 Encrypted Public Recording (DEPR) inhibits mass surveillance by requiring a court subpoena 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[12] information technology can be a very powerful tool for catching criminals using DEPR because it can provide principled methods and technology for processing large amounts of pervasively inconsistent information.[13]

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

Available technology alternatives are summarized in the following table:

CyberLocalism	CyberTotalism
Enterprise and Citizen Islets™ Information Integration[15] • RAM-processor package encryption • Every-word tagged architecture • Strong biometric authentication • Auditable public keys for citizens and IoT ownership	**Datacenterism**[5][7][15][17][19][22] • Ever increasing consumer surveillance for better targeted advertising • Security services have access to all datacenter information of companies domestically domiciled (with gag orders)
Distributed Encrypted Public Recording(DEPR) • Accessible by individualized court subpoena • Totally inaccessible after a set time period (enforced by encryption)	**Mandatory backdoors for all IoT**[2][15][24] Each nation surveils its own citizens • Includes body-sensor computer networks • Potential security vulnerabilities after security services have taken control of a device

Available technology alternatives

Acknowledgements
This article has greatly benefited from detailed critiques and organizational suggestions of Alan Karp and Andy Rosenbloom, editorial suggestions of Dennis Allison and Henri Gouraud, comments by Chip Morningstar, conversations with Jeff Rulifson and Erik Meijer and suggestions of Ron Rivest and Peter Neumann. John Dalton provided design and editorial consulting.

The author's Erlang keynote address *Actors for CyberThings*[15] covers some of the material in this article.

References

[1] 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.

[2] James Areddy. *China Pushes to Rewrite Rules of Global Internet.*

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

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

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

[7] Rian Gallagher. *Revealed: How DOJ Gagged Google over Surveillance of WikiLeaks Volunteer*. The Intercept. June 20, 2015.

[8] Ryan Gallagher and Glenn Greenwald. *How the NSA plans to infect 'millions' of computers with malware. The Intercept.* March 12, 2014.

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

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

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

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

[13] 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.

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

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

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

[17] Jenna McLaughlin *Edward Snowden Explains Why Apple Should Continue To Fight the Government on Encryption*. The Intercept. July 31, 2015.

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

[19] Ewen MacAskill. *NSA paid millions to cover Prism compliance costs for tech companies.* The Guardian. August 23, 2013.

[20] Jens Masuch and Manuel Delgado-Restituto. *Ultra Low Power Transceiver for Wireless Body Area Networks.* Springer. 2013.

[21] Bill Marczak, *et. al.*. *China's Great Cannon*. University of Toronto. April 10, 2015.
[22] Salvador Rodriguez. *NSA 'Equation' Fallout: Experts Say Damage To US Tech Firms Could Top $180B* International Business Times, February 15, 2015.
[23] Jeremy Scahill and Josh Begley. *The CIA Campaign to Steal Apple's Secrets*. The Intercept. March 10, 2015.
[24] Robert Scheer. *They Know Everything About You: How Data-Collecting Corporations and Snooping Government Agencies Are Destroying Democracy* Nation Books. 2015.
[25] Eric Schlosser. *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*. Penguin Books. 2014.
[26] Sam Thielman. *Cybersecurity bill could 'sweep away' internet users' privacy, agency warns.* The Guardian. August 3, 2015.
[27] Daniel Thomas. *Huawei does not pose risk to UK national security, report finds.* Financial Times. March 31, 2015.