Security without IoT Mandatory Backdoors

Carl Hewitt

Security without IoT Mandatory Backdoors

Using Distributed Encrypted Public Recording to Catch & Prosecute Suspects

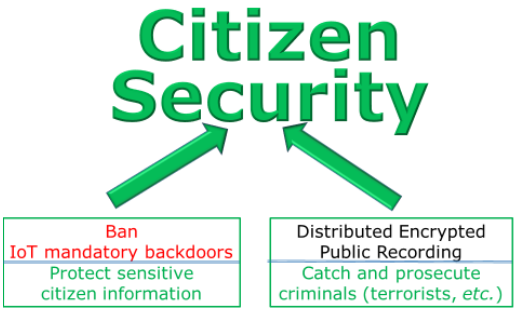
Our greatest enemy is our own apathy.
Bill Mullinax

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

This article explains how Citizens' civil liberties can be preserved by banning Internet of Things (IoT[i]) mandatory backdoors while at the same time effectively catching and prosecuting suspects (such as alleged "terrorists").

IoT devices are becoming pervasive in all aspects of life including personal, corporate, government, and social. Adopting IoT mandatory backdoors ultimately means that security agencies of each country surveil and control IoT in their own country and perhaps swap surveillance information with other countries.[7][14][35][41][42] Burr-Feinstein[3] have proposed that it must be possible for security agencies to be able to secretly access and take control of any individual IoT device. However adopting their proposal would make it very difficult to prevent security agencies from accessing and controlling large numbers of devices and abusing their surveillance and control capabilities.[13][14][35][41][42][49] Also, adopting IoT mandatory backdoors would be corrosive to civil liberties because any IoT device could be secretly accessed and controlled without any awareness by those using the device.[14][41][42][49] 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.[1][13][14][41][42][49]

> A ***backdoor*** is means by which an IoT device can be secretly accessed and/or 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 informed users of the device.



Distributed Encrypted Public Recording (DEPR) is system in which distributed[ii] 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

[i] including body-sensor computer networks[31], cell phones[2], bedroom TVs[26], PCs[14], Internet LEDs, car, and soon brain implants[8][10][38].

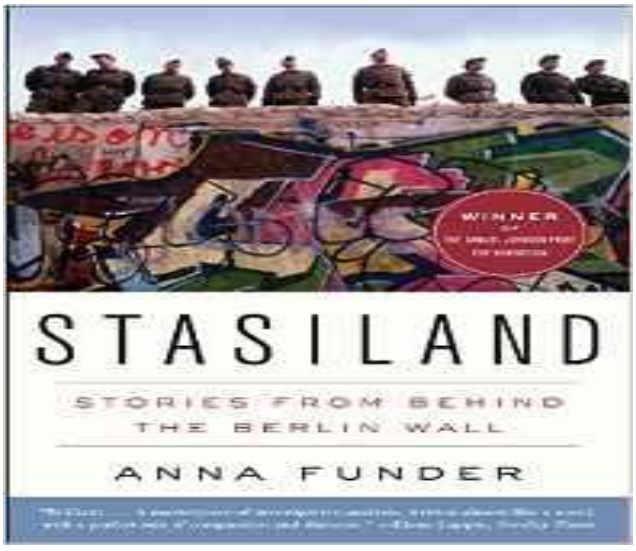
[ii] for example stores, restaurants, cell towers, sports events, parks, and theaters.

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 and control. Advanced Inconsistency Robust[20] information technology can be a very powerful tool for catching and prosecuting suspects 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.

This above proposal aims to balance the Constitutional requirement to protect citizens' civil liberties and for law enforcement to catch and prosecute suspects (such as alleged "terrorists"). It would uphold the U.S. Constitution's Fifth Amendment right against self-incrimination by prohibiting mandatory IoT backdoors that could provide access to sensitive personal information. At the same time, it would not prohibit access to "distributed encrypted public recording" (such as videos in public places, all financial transactions, and locations of cell phones from cell towers) so all recorded activities except those in personal IoT devices could be subpoenaed.

Mass Surveillance and Control

Mass surveillance by the US Government has been extraordinarily successful (in the narrow military sense) 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.[24][29] 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.[5][6][42] 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 and control has a long history of being used to 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), and Erich Mielke (Stasi)[12] terrified 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.[13][46][49] The exact nature of interconnectivity between corporate datacenters and government security datacenters is in each case a closely guarded corporate secret that can be enforced by government gag orders.[13][46][49]

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.
- President Reagan authorized the beginnings of mass surveillance of US and (more broadly) foreign citizens in Executive Order 12333.[34]
- The administration of President George W. Bush (spearheaded by Dick Cheney, David Addington and John Yoo) authorized even greater mass surveillance.[34]
- Mass surveillance was continued and extended during the initial phases of the Obama administration.[2][5][13][14][29][41][34]
- Future Presidents using mass surveillance and control enabled by IoT mandatory backdoors could do immense damage to civil liberties.[15][18][24][33][35][41][46][49]

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.[6][46][49] 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[30]) thereby making corporate engineers and executives *increasingly complicit in mass surveillance and control*.[6][22][30][46] Furthermore, businesses can be harmed by their inability to change datacenter operations because it would disrupt[42] government surveillance and control. Government security agencies can enforce uniformity of datacenter operations across companies to increase the effectiveness and efficiency of their surveillance and control operations at the cost of inhibiting innovation and flexibility of company operations.[6][30][46]

Mass surveillance using 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:[7][42]

- "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.

Economic Consequences of Foreign Mass Surveillance

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.[6][13][16][30][39][41][44][46][49] 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.[6][39] "*In short, foreign customers are shunning U.S.*

companies."[6] These losses could be increased tenfold if they spread to manufacturers that include IoT connected to their datacenters, which stands to include almost *everything*.

Infeasibility of auditing foreign-domiciled datacenters

- A foreign-domiciled company is subject to foreign laws, gag orders, and other pressures to cooperate with foreign intelligence agencies.[7][15][16][41][42][49]
- 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 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.[5][6][24][45][47] Likewise, every government can require that IoT sold in their country do not have backdoors accessible to other governments.[5][6][28][46][47][49]

Economic losses of Internet companies due to surveillance using 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 or use IoT devices (just about everything manufactured) that communicate citizens' sensitive information with the company's datacenters.[13][41][49] For example, the Advocate General of the European Court of Justice stated: [5]

- "*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].*"

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

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.[5][6][46]

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.[5][6][41][47][49]

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.[46][47][48][49][49] Growing mistrust of the security of sensitive citizen information stored in datacenters of foreign-domiciled corporations is a severe problem for multi-nationals.[5][6][28][39][41][42][46][49][49] 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.[5][6][46]

> Corporations need to understand that sensitive citizen information is not always a corporate asset and instead can be a toxic corporate liability.[5][6][7][11][22][29]

IoT in all manufactured devices

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.

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.[8][10][38]

Power of IoT Backdoors[21][31]

Mandatory IoT Backdoor Proposal

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 ask a judge to order Apple to write software to give the government the ability to decrypt all information on the iPhone (which is technically called creating a "backdoor")? Also should government have the power to ask a judge to prohibit importation of Samsung phones for which Samsung cannot decrypt all messages that have been sent or received on the phone?

Senators Richard Burr and Dianne Feinstein have proposed legislation for mandatory IoT backdoors as follows:[3]

> *covered entities*[iii] must provide unencrypted information and technical assistance[iv] to the government pursuant to a court order.[v]

The above proposal requires that it must be possible to secretly take control of any IoT device while it is connected to the Internet and incrementally access all information on the device as it is decrypted which can be accomplished as follows:

> 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. A device must be able to be secretly taken-over and 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 cryptography).

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.

Mandatory backdoor technology can build on already developed CIA/GCHQ/NSA surveillance and control technology including QUANTUM, SMURF, TURBINE, TURMOIL, UNITEDRAKE, WARRIOR PRIDE, and VALIDATOR.[14][42] The equivalent of a (preferably unique) public key can be installed by the manufacturer on each a device.

[iii] *Covered entities* include ***all*** of the following:

1. device manufacturers, software manufacturers, electronic communication services, remote computing services, providers of wire or electronic communication services, providers of a remote computing services, and entities that provide a product or method to facilitate a communication or the processing or storage of data.
2. providers of remote computing service or electronic communication service to the public that distribute software for products, services, or applications

[iv] in order to secretly access and take control of IoT devices

[v] The Burr-Feinstein proposal is an attempt to legislate IoT mandatory backdoors extending current attempts by the government to use the All Writs Act, which has been ruled unconstitutional by a court (but the ruling is being appealed by the government).[37]

The private key can be split held by government authorities of the nation in which the device is to be operated.[48] 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.[43]

IoT Mandatory Backdoor Consequences

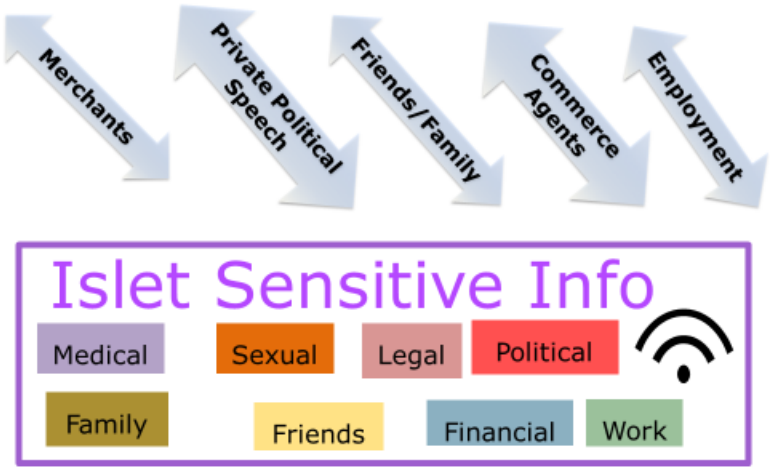
The mandatory backdoor proposal for all IoT (including devices that electronically communicate with IoT) can influence countries to require that IoT products sold in a country must be audited against backdoors available to *other* countries.[6][41][46][48][49] It is technically much easier to audit against *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[17] and kinetic responses to cyberattacks because of potential vulnerabilities in the many different government backdoor implementations.[32][41][47][49] Also, mandatory backdoors can increase the security risks to military equipment because they might be exploited by enemy forces. Furthermore, IoT mandatory backdoors can enormously increase the power of government security agencies.[12][41][42][46][49][49]

Protecting Sensitive Citizen Information

Sensitive information is nonpublic information revelation of which can potentially harm a citizen, such as 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, such as 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.[19]

CyberLocalism is a system in which a citizen's sensitive information is stored locally in their own equipment (without backdoors) – *the antithesis of both Datacenterism and CyberTotalism*.[21][46]

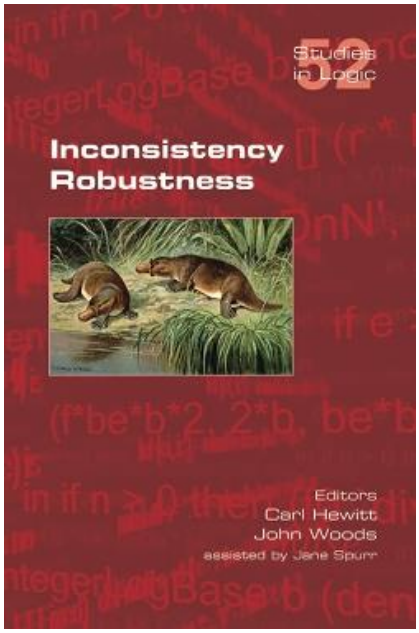
CyberLocalism might never come to fruition unless it is supported by a business model that is more efficient and effective than the currently popular system of Datacenterism based on the consumer surveillance and influence business model.[21] Consequently, the Standard IoT™ international, nonprofit standards 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, such as routers, body-sensor computer networks[31], 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 citizens' IoT 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.*)[4], *Social* (schedule, friends, family, *etc.*), and *Work* (contacts, schedule, colleagues, *etc.*) [21]

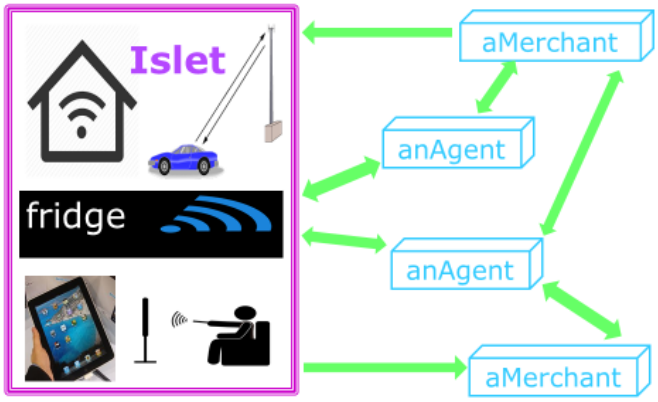
An Islet can run on multiple citizen devices such as cell phones, refrigerators, insulin pumps, bedroom TVs, brain implants, and home routers. These devices are connected only intermittently and some of them may fail permanently. Consequently an Islet must deal with asynchronously-arriving information from various devices and from the outside Internet. Fortunately, Actors[20] 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).[20]

Also, Islet information can be backed up elsewhere automatically encrypted using the citizen's public keys including using 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[20] 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

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.

Cyberlocalism advantages over datacenterism:[13][28][43]
Cyberlocalism offers lower communications cost because it is not necessary to always communicate with datacenters. It can also provide faster response and more robustness because local operations can be faster and more reliable than always interacting with potentially overloaded datacenters. Better protection of a citizen's sensitive information is possible because it is not always available in datacenters accessible by security agencies. 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.[21] Further cyberlocalism can provide improved coordination between customers and merchants with more relevant and less intrusive advertising as well as better coordination between a customer and competing merchants

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

Security of IoT devices

Greater security of citizens' IoT devices is required because currently state-sponsored and other intruders can secretly access and take control of almost any citizen's personal IoT devices.

An IoT device needs 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.[vii]

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. 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 consortia and proprietary corporate IoT standards.

How to Increase IoT Security

- Public keys for device ownership
- Authenticated public keys for citizens
- Bio-authentication of users
- Hardware protection of software Actors (applications as well as their Java and C/C++ objects) using the following:
  - RAM-processor package encryption (*i.e.* all traffic between a processor package and RAM is encrypted using a uniquely generated key when a package is powered up and which is invisible to all software) to protect an app (*i.e.* a user application, which is technically a process) from operating systems and hypervisors, other apps, and other equipment, for example 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 (for example 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.

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.[20][21]

[vii] For efficiency reasons, most communication can be performed using symmetric keys encrypted/signed by public keys.

Going Forward

> *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.[20]

Advertising Competitive Race to the Bottom

In a competitive race down an ethical abyss, many Internet companies depend on ever greater surveillance in order to better target consumers for advertising.[12][22][24] *However, a nation's security depends on limiting surveillance of their citizens by foreign security agencies enabled by Internet companies domiciled in other nations*.[11][13][28]

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 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.[7][20] Since almost all manufactured exports will soon include IoT, we can expect that losses to US industry will be enormous unless drastic changes are made.

Eventual fate of foreign datacenters with sensitive citizen info

1. **Datacenter Info Localization**: Citizens' datacenter information must be stored domestically so that 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.

Going forward, security agencies have proposed mandatory backdoors for all IoT so that they can always be able to surveil and control anything and everything that might be deemed necessary by the government.[21][41][49] As indicated by NSA Director Mike Rogers, mandatory backdoors mean that security agencies of each country surveil and control citizens in their own country[21] 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 and control capabilities.[20][41][49] Of course, any attempt to *change* the device's application behavior can introduce additional vulnerabilities.

The right against self-incrimination by body-sensor computer networks[31] will be become increasingly important. Since personal IoT of a citizen can be an essentially part of the person, mandatory backdoors can compel testimony of the most intimate kind.

Consequently, IoT mandatory backdoors could become a severe threat to citizens' rights. Just the public awareness itself that any IoT device could be secretly accessed and controlled by security agencies could be extremely corrosive to social arrangements.[5][6][14][32][41][49] 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.[21] It was extremely abusive to use people's sensitive information against them as was done by the Stasi[19], Hoover's FBI COINTELPRO, *etc*.[12] Because of improving information technology using IoT will become ever more important.[5][6][7][22][24][41][49] Adopting Islets would go a long way toward protecting citizens' sensitive information against both government and corporate abuse.[21]

IoT mandatory backdoors consequences

- security agencies of each country surveil and control IoT in their own country and perhaps swap surveillance information with other countries.[14][32][49]
- make it very difficult to prevent security services from accessing and controlling large numbers of devices and abusing their surveillance capabilities[12][13][14][32][41][49]
- corrosion of civil liberties because any IoT device could be secretly accessed and controlled without any awareness of those present[12][14][18][32][41][49]
- massive corruption as a result of sensitive IoT information spreading from local security agencies to their political supervisors[18][23][41][49]
- 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.[1][13][21][32]

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.[7][28][30][39][41][42][46][49] One outcome is for 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.[5][6][7] A multinational could take the proceeds of the IPO from 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.[20]

[viii] for example Alibaba, Amazon, Apple, Cisco, Facebook, Google, HP, IBM, Intel, LG, Microsoft, Panasonic, Samsung, and Yahoo.

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."

Distributed Encrypted Public Recording (DEPR) inhibits mass surveillance and control by requiring a court warrant to access encrypted information recorded by distributed parties with a write-only log kept for all accesses thereby making mass surveillance and control more costly, both politically and economically. Inconsistency Robust[20] information technology can be a useful tool in developing new technology for more effectively catching and prosecuting suspects using DEPR that has pervasively inconsistent information.[20]

Arguments Against
IoT Mandatory Backdoors

- Economic
  - cripple IoT market because citizens shun devices as government spyware
  - hamper IoT exports and imports because foreign devices will have backdoors potentially available to foreign security services
- National defense
  - auditing citizen IoT against backdoors of foreign intelligence agencies becomes more difficult
  - auditing government IoT against backdoors of foreign military forces becomes more difficult
- Loss of civil liberties due to mass surveillance and control
- Increased corruption and breakdown of societal trust
  - Stasiland
  - FBI COINTELPRO
  - Contemporary China and Russia
- Against medical ethics to mandate backdoors in medical IoT, for example pacemakers and soon brain implants
- Security vulnerabilities become greater as the number of IoT devices controlled by others grows larger, for example use by local police departments

In opposition to the Burr-Feinstein legislative proposal[3] discussed above, I propose the following legislative principles to help guide the law in safeguarding our civil liberties:

> "The U.S. government or any of its political subdivisions, including a state or its political subdivisions, may not order or coerce a manufacturer, seller, developer, or provider of computer hardware, software, or device made available to the general public to design, alter, or modify the related security features in order to allow a federal or state agency to obtain information stored in such a device or provide the ability to decrypt information encrypted therein."[ix]

[ix] *cf.* [27]

A new commission, the IoT Security Commission (ISC), is needed to enforce the prohibition against mandatory backdoors in citizen IoT and to regulate Distributed Encrypted Public Recording (DEPR) that would have jurisdiction over all providers of IoT equipment in the US:[20] ISC would require that every kind of IoT device be audited using operational bi-simulation against a publicly available operational specification overview by mandating 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. ISC would provide registration and oversight of firms providing cyberaudit services ("*cyberauditors*") including specific processes and procedures for compliance cyberaudits, inspect and police cyberaudit conduct and quality control. Cyberauditing companies would be prohibited from providing non-audit services (for example consulting) for the same clients.

Sleepwalking into Cybertotalism[40]

"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."

Edward Snowden

Right against self-incrimination

- Citizens' IoT devices should not require that they surrender control of their personal devices or sensitive information, 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.

Available alternatives

Islets[TM][21]	**Datacenterism**[7][13][16][30][33][39][46][49]
Business model[12][21] Islet-agent-merchant brokering[13]	**Business model**[12][20][50] Ever increasing consumer surveillance for better targeted advertising
Security model[12][13][21] ○ RAM-processor package encryption to protect applications from memory-bus devices, 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**[13][33][49] 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)**[21] • 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**[7][14][18][33][49] • Surveil thoughts including brain implants • Any IoT device can be accessed and controlled if connected to the Internet • Includes body-sensor computer networks • Each nation surveils and controls its own citizens • Potential security vulnerabilities after security services have taken control of a device

Conclusion

The issue of mandatory IoT mandatory backdoors is one of the most momentous constitutional issues that the nation has ever faced. A broadly-based Cyber Study Commission[x] (with power of subpoena) should be established to hold public hearings, investigate, and issue a final report in a year's time. The Commission should be chaired by a distinguished constitutional scholar[xi] and take its membership from the following:

Brain prosthetic researchers
Civil liberties organizations
Civil rights organizations
Computer scientists
Legal scholars

Industry
- Information Technology
- Manufacturing

Medical societies
National academies
Professional societies

Testimony should be heard from a broad spectrum of society including the following:

Executive Branch
- Commerce
- Defense
- Homeland Security
- Justice
- National Intelligence Council
- NIH
- NIST
- NSF
- OSTP
- State

Commissions
- FCC
- FTC

American Academy of Neurology
American Bar Association
American Civil Liberties Union
American-Arab Anti-Discrimination Committee
American Anthropological Association
American Historical Association
American Jewish Committee
American Judges Association
American Medical Association
American Medical Informatics Association
American Press Association
American Psychiatric Association
American Psychological Association
American Sociological Association
Association of Computing Machinery
Association of Prosecuting Attorneys
Center for Constitutional Rights
Electronic Frontier Foundation
Electronic Privacy Information Center
Internet Association
League of United Latin American Citizens
New America Foundation
Southern Poverty Law Center

[x] The Cyber Study Commission needs to be much broader in scope and more broadly representative that the recently appointed Commission on Enhancing National Cybersecurity.[9]

[xi] such as someone of the caliber of Harvard Dean Martha Minow

On March 11, 2016 at SXSW, President Obama warned that another incident like the recent one at San Bernardino, could panic Congress into passing legislation extremely dangerous to civil liberties (such as the Burr-Feinstein proposal[3]). Consequently, the President should appoint the Cyber Study Commission described above as soon as possible so that there will be an opportunity for a full and complete consideration of the issues.

Judicial Ruling[37]

"How best to balance those interests is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago. But that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive."

Judge Magistrate James Orenstein

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 Timothy Edgar, Ron Rivest and Peter Neumann. John Dalton provided design and editorial consulting.

The author's Erlang keynote address *Actors for CyberThings*[21] covers some of the material in this article.

The Author

Professor Carl Hewitt is the founder of the field of Inconsistency Robustness, i.e., the science and engineering of large systems with continual, pervasive inconsistencies (a shift from the previously dominant paradigms of inconsistency denial and inconsistency elimination). He is currently Board Chair of the International Society for Inconsistency Robustness (iRobust™). Previously, he was Program Chair of international symposia on the subject at Stanford in 2011 and 2014. The standard text on the subject is Inconsistency Robustness[20][36] for which Hewitt is co-editor and a contributor. Operational aspects of Inconsistency Robustness are addressed using the Actor Model of computation and inferential aspects using Direct Logic™.

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. 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 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. He is also known for the design of Planner, the first programming language based on pattern-invoked procedural plans, which influenced the development of Prolog-like programming languages and subsequent ultra-concurrent programming languages making used of Logic Programming constructs based on the Actor Model.

His homepage is https://plus.google.com/+CarlHewitt-StandardIoT

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] 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.

[3] Richard Burr and Dianne Feinstein. *Compliance with Court Orders Act of 2016* Discussion Draft. April 8, 2016.

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

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

[6] 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.

[7] 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.

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

[9] Michael Daniel, Ed Felten and Tony Scott. *Announcing the President's Commission on Enhancing National Cybersecurity* The White House. April 13, 2016.

[10] 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.

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

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

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

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

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

[16] Jennifer Granick. *OmniCISA Pits DHS Against the FCC and FTC on User Privacy.* Just Security Blog. December 15, 2015.

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

[18] Christine Hauser. *Denver Police Caught Misusing Databases Got Light Punishments, Report Says.* New York Times. March 17, 2016.

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

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

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

[22] Cullen Hobak. *Terms and Conditions May Apply*. Phase 4 Films. 2013.
[23] Justin Jouvenal. *The new way police are surveilling you: Calculating your threat 'score'*. Washington Post. January 10, 2016.
[24] Steve Kroft. *The Data Brokers: Selling your personal information.* 60 Minutes. March 9, 2014.
[25] Edward Lee. *Swarm Boxes*. SwarmLab UC Berkeley. March 19, 2015.
[26] John Leyden. *Hey, does your Smart TV have a mic? Enjoy your surveillance, bro.* The Register. May 10, 2014.
[27] Ted Lieu. *Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016.*
[28] Jenna McLaughlin *Edward Snowden Explains Why Apple Should Continue To Fight the Government on Encryption*. The Intercept. July 31, 2015.
[29] Ellen Nakashima. *With a series of major hacks, China builds a database on Americans.* Washington Post. June 5, 2015.
[30] Ewen MacAskill. *NSA paid millions to cover Prism compliance costs for tech companies.* The Guardian. August 23, 2013.
[31] Jens Masuch and Manuel Delgado-Restituto. *Ultra Low Power Transceiver for Wireless Body Area Networks.* Springer. 2013.
[32] Bill Marczak, *et. al.*. *China's Great Cannon*. University of Toronto. April 10, 2015.
[33] Theresa May (UK Home Secretary). *Draft Investigatory Powers Bill.* Presented to Parliament. November 2015.
[34] Jane Mayer. *The Dark Side*. Doubleday. 2008.
[35] Jenna McLaughlin and Zaid Jilani. *We Asked NSA's Privacy Officer If U.S. Spying Powers Are Safe With Donald Trump. Here's What She Said.* The Intercept. March 24, 2016.
[36] JJ Meyer. *Review of Inconsistency Robustness.* College Publications. 2016. http://collegepublications.co.uk/review/lgc00030.pdf
[37] Judge Magistrate James Orenstein. *Memorandum and Order.* 15-MC-1902 (JO). February 29, 2016.
[38] Abby Philip. *A paralyzed woman flew an F-35 fighter jet in a simulator — using only her mind.* Washington Post. March 3, 2015..
[39] Salvador Rodriguez. *NSA 'Equation' Fallout: Experts Say Damage To US Tech Firms Could Top $180B* International Business Times, February 15, 2015.
[40] Arundhati Roy. *Edward Snowden meets Arundhati Roy and John Cusack: 'He was small and lithe, like a house cat'* The Guardian. November 28, 2015.
[41] Charlie Savage. *Obama Administration Set to Expand Sharing of Data That NSA Intercepts.* New York Times. February 25, 2016.
[42] Jeremy Scahill and Josh Begley. *The CIA Campaign to Steal Apple's Secrets*. The Intercept. March 10, 2015.
[43] Eric Schlosser. *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*. Penguin Books. 2014.
[44] Scott Shane and Colin Moynihan. *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s* NY Times. September 1, 2013.
[45] Dave That, Vint Cerf, *et. al. Request for the Allowance of Optional Electronic Labeling for Wireless Devices* Letter to US FCC. RM11673. 2015.
[46] Sam Thielman. *Cybersecurity bill could 'sweep away' internet users' privacy, agency warns.* The Guardian. August 3, 2015.
[47] Daniel Thomas. *Huawei does not pose risk to UK national security, report finds.* Financial Times. March 31, 2015.
[48] US National Security Council. *Draft paper on technical options for the encryption debate.* Leaked. September 2015.
[49] Cyrus R. Vance, Jr. *Written Testimony Before the United States House of Representatives Committee on the Judiciary*. March 1, 2016.
[50] Shoshana Zuboff. *Big other: surveillance capitalism and the prospects of an information civilization.* Journal of Information Technology Vol. 30. 2015.