SSRN WP 2836282

Islets Protect Sensitive IoT Information

Verifiably ending use of sensitive IoT information for mass surveillance
fosters (international) commerce

Carl Hewitt
https://plus.google.com/+CarlHewitt-StandardIoT/

Islets is a system for citizens to coordinate with IoT devices and other citizens while protecting their sensitive health, legal, political, and social information and fostering (international) commerce by enabling conclusive verification that foreign governments are no longer conducting mass surveillance using IoT manufactured products and Internet company service provider datacenters[Chappell 2017; Gunaratna 2017; Enck 2010; Leyden 2014; Monroe 2017].

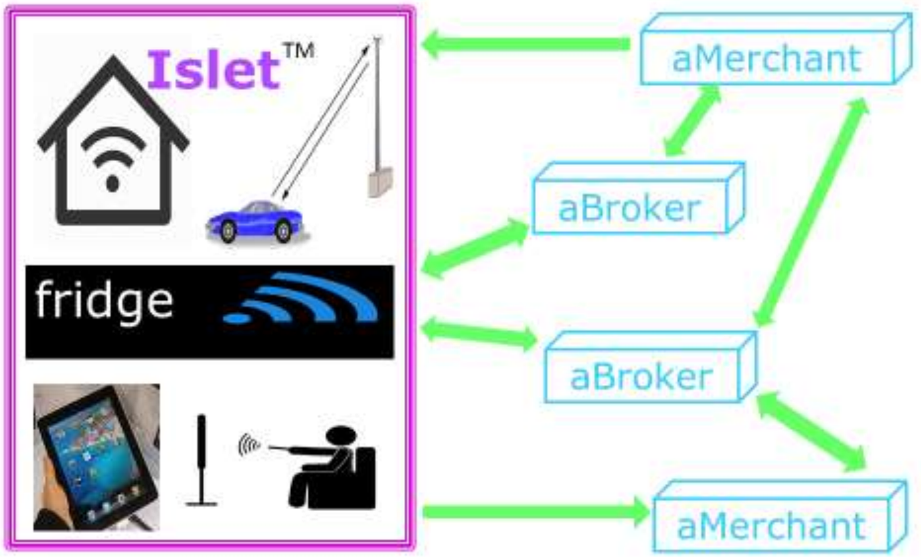
IoT poses extreme security and privacy challenges for sensitive personal information, including psychological, sexual, social, financial, legal, and medical. Enormous amounts of sensitive information that can be used against citizens is being stored in datacenters controlled by foreign-domiciled companies[Beeler 2017; Chappell 2017; Disconnect 2015; Gunaratna 2017; Leyden 2014; Monroe 2017] and extensively sold on multiple markets by data brokers[Enck 2010; Herbert 2016; Martinez 2016].[16] Within 10 years, hologlasses (holographic glasses) are projected to become as common as cell phones because they offer heads-up, hands-free, transparent operation[Mackie 2016; Mundy 2016]. Consumer health and medical IoT involve the some of the most sensitive of information that can be used against citizens. For example, pacemakers and insulin pumps are becoming ever more common. Further out, 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 [DARPA 2016]. Many workers and military personnel may someday not be competitive if they lack a brain prosthetic[Cott 2015; Philip 2015].

IoT will soon be in almost all manufactured devices thereby threatening the economic survival of tans-national manufacturers as well as Internet companies because of their current Internet business model of storing the most sensitive of personal information in their datacenters from IoT devices. Cyberspace Administration of China, European Court of Justice and other national governments have announced their intention to verifiably end mass surveillance of their citizens by foreign governments using datacenters of foreign-domiciled companies[Beeler 2017; Bot 2015; Castro and McQuinn 2015; China National People's Congress 2016; Farrell and Newman 2016; Mozur and Perlez 2016; Hewitt 2016b] because information stored in the datacenters of foreign-domiciled corporations can at some future time become accessible to the government of the country in which the company is domiciled. [Packel 2017] Consequently, companies that store sensitive information in their datacenters must be domestically incorporated to be able to verify that foreign governments do not have bulk access to the information. Islets are a means for trans-national companies (including both IoT manufacturers and Internet service providers) to escape this trap by storing sensitive information of users' IoT devices in Islets and storing only non-sensitive information in their datacenters[Hewitt 2016b].

Sensitive information can be stored locally in Islets on users' own equipment encrypted with user keys and can be backed up elsewhere encrypted using users' keys. Furthermore, users can share Islet information that they select with other parties -- encrypted with the public keys of other parties so that it be read only by the intended party.

Islets can improve information coordination over current systems that cannot coordinate among numerous competing services (such as Facebook and Google) and numerous fiercely competing merchants (such as Amazon, Home Depot, and Walmart using multiple IoT devices from competing manufacturers (such as LG, Nest, Samsung, and Whirlpool). Islet-facilitated coordination can include integration of commerce (such as home, retail, food, travel, and auto), wellness (such as recreation, biometrics, nutrition, exercise, spirituality, medical, and learning), finance (such as banking, investments, and taxes), IoT (such as food management, security, energy management, infotainment, transportation, and communication), social (such as schedule, friends, and family), and work (such as contacts, schedule, and colleagues).

Islets can provide lower communications cost than current systems because it is not necessary for users and their IoT devices to always communicate with datacenters[Burnside, Clarke, Mills, Maywah, Davadas, and Rivest 2002; Hewitt and Woods assisted by Spurr 2015; Lee 2015]. Islets also can provide faster response and more robustness because local operations can be faster and more reliable than being required to always use communication links with potentially-overloaded remote datacenters.



Islet Coordinating with Agents and Merchants Business Model

Islets need a convenient, effective, high-profitable business model, which must be more effective and efficient than the current datacenters system based on consumer surveillance to improve advertising targeting. Instead, an Islet running on a consumer's equipment can seek out and help evaluate appropriate offers from commerce agents. Such commerce agents can earn commissions and fees from merchants when the referral is exercised. Consequently, merchants will no longer be burdened by having to pay for *grossly inefficient* advertising that annoys potential customers. Instead, businesses can provide their information to commerce agents that aggregate and package it for users' Islets to be used in evaluating offers that can be filtered and ranked according to citizen needs and preferences. All of the convenience currently available through individual company access points must be improved in effectiveness and response time including scalable search and operations that can query commercial datacenters (such as Amazon, Facebook, Google, and LinkedIn) as well as other Islets. (See the appendix “Implementation of Islets” after the acknowledgements of this article).

Outside of citizens' Islets information protected against self-incrimination, governments (through subpoena) will be able to obtain sufficient information for law enforcement including financial transactions, physical movements outside the home, and cell tower tracking information.

Mass surveillance using datacenters of foreign-domiciled companies.

Because Islets store sensitive citizen information outside of datacenters, they can help the European Court of Justice (ECJ) in its avowed goal to end mass surveillance of EU citizens using datacenters of foreign-domiciled companies. ECJ has backed up [Bot 2015]:

- "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 EU fundamental rights]."

According to Yahoo,

> "Recent new stories have provoked broad speculation ... about the activities and representations of the U.S. government, including those made by the Government in connection with negotiating Privacy Shield with the European Union. That speculation results in part from lack of transparency and because U.S. law significantly constrain–and severely punish–companies' ability to speak for themselves about national security related orders even in ways that do not compromise U.S. government investigations."[Bell 2016]

Advocate General Bot of European Court of Justice (ECJ)

Should confidence be lost in the assurances made by US in the Privacy Shield agreement, then pressure will increase for EU to demand conclusive verification that datacenters of foreign-domiciled companies are not facilitating mass surveillance of EU citizens. In this regard, ECJ is a canny and powerful player[Farrell and Newman 2016], which ruled on December 21, 2016 that the "general and indiscriminate retention" of data about people's communications and locations is inconsistent with privacy rights. The court further stated that the "highly invasive" bulk storage of private data "exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society." It may soon rule that mass surveillance of Europeans by foreign governments using datacenters of foreign-domiciled companies must *verifiably* cease. Such a ruling would be binding on all EU countries and would overthrow Privacy Shield agreements that currently allow foreign-domiciled companies datacenters to hold sensitivie information of EU citizens.

There are similar concerns about the UK. According to Big Brother Watch, "The passing of the [UK] Investigatory Powers Act has fundamentally changed the face of surveillance in this country. None of us online[1] are now guaranteed the right to communicate privately and, most importantly, securely."[MacAskill 2016] The bill explicitly allows mass breaking into foreign targets by GCHQ, which works very closely with NSA. Any warrants issued to a company to decrypt users' data can come with a gagging order, forbidding the firm from discussing it. According to the Verge, "Taken as a whole, it's hard to see the Investigatory Powers Bill as anything other than a reshaping of the concept of private civil society {because local constables will have access to the information collected}."[Vincent 2016] According to the Guardian, "{Local government} councils were given permission to carry out more than 55,000 days of covert surveillance over five years, including spying on people walking dogs, feeding pigeons and fly-tipping."[Asthana 2016]

[1] worldwide including the press, lawyers, psychiatrists, doctors, clergy, and Members of Parliament

According to Congressperson Michael Capuano:

> *the Federal Trade Commission fined the makers of Vizio televisions $2.2m for collecting viewing data on 11 million consumers without telling them. If you owned a Vizio TV it could hear you even when turned off – and it could see you too! Information was gathered and shared with retailers to refine sales techniques and better target consumers.*
>
> *Samsung has admitted that they were conducting similar spying with their televisions and recently a company selling "smart" teddy bears was exposed for collecting 2 million voice recordings of children and parents.* [Capuano 2017]:

Sensitive medical information is of particular concern. According to the Guardian [Thielman 2017]:

> *Your medical data is for sale – all of it. Adam Tanner, a fellow at Harvard's institute for quantitative social science and author of a new book on the topic, "Our Bodies, Our Data", said that patients generally don't know that their most personal information – what diseases they test positive for, what surgeries they have had – is the stuff of multibillion-dollar business.*
>
> *But although the data is nominally stripped of personally identifying information, data miners and brokers are working tirelessly to aggregate detailed dossiers on individual patients; the patients are merely called "24601" instead of "Jean Valjean".*
>
> *But other forms of data, such as information from fitness devices and search engines, are completely unregulated and have identities and addresses attached.*
>
> *None of this technically violates the Health Insurance Portability and Accountability act, or HIPAA, Tanner writes. But the techniques do render the protections of HIPAA largely toothless. "Data scientists can now circumvent HIPAA's privacy protections by making very sophisticated guesses, marrying anonymized patient dossiers with named consumer profiles available elsewhere – with a surprising degree of accuracy*.

According to Ewen MacAskill,

> *We are in a really desperate place. Britain last year passed the Investigatory Powers Act, which allows Intelligence Agencies all the things that they we doing that were previously illegal to become legal and also gives them powers that they didn't have before so that UK has enacted some of the most draconian surveillance laws ever enacted in a Western democracy. What was really disappointing was that in Germany the Bundestag passed similar legislation last year as well. The same in France and world-wide*. [Shore 2017]

According to Edward Snowden [Guardian video posted June 9, 2013]:

> *There will be a time when policies will change. The only thing that restricts the activities of the surveillance state are policy. Even our agreements with other sovereign governments. We consider that to be a stipulation of policy rather than a stipulation of law. And because of that, a new leader will be elected. They'll flip the switch, say that because of the crisis, because of the dangers that we face in the world, you know, some new and unpredicted threat, we need more authority. We need more power. And there will be nothing the people can do at that point to oppose it, and it will be turnkey tyranny.*

Secret orders have been issued allowing security agencies to conduct surveillance worldwide using domestically incorporated datacenters with gag orders that this surveillance not be disclosed[Bot 2015; Castro and McQuinn 2015; Farrell and Newman 2016; Menn 2016; Vincent 2016] According to the Information Technology and Innovation Foundation, "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" with the result "In short, foreign customers are shunning U.S. companies." [Castro and McQuinn 2015] These losses could be increased tenfold if foreign-domiciled IoT manufacturers follow their current plan of storing sensitive information in their datacenters because of the size of the manufacturing industry and because the IT industry also plans to continue their practice of storing sensitive citizen information in their datacenters.

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) thereby making corporate engineers and executives increasingly complicit in government-run security operations.[Bell 2016; Castro and McQuinn 2015; Hobak 2013; Menn 2016] Furthermore, business flexibility and innovation can be harmed by the inability to change datacenter operations because any changes might disrupt government surveillance and control. Governments can enforce uniformity of datacenter operations across companies to increase the effectiveness of their surveillance and control operations at the cost of inhibiting innovation and flexibility of company operations [Castro and McQuinn 2015].

In an attempt to maintain their freedom of action and to preserve their business model based on targeted advertising, companies have pushed back against datacenter bulk access by governments[Bell 2016]. However, even if a company can temporarily fend off government bulk access, it cannot provide assurance that the government will not later gain access to information currently stored in its datacenters. There is no way to verify that information once stored in a company's datacenters will not be accessible in the future. Furthermore, a foreign-domiciled company is subject to its government's laws, gag orders, and other forms of pressure to cooperate[Beeler 2017; Bell 2016; Hewitt and Woods assisted by Spurr; Menn 2016; Vincent 2016]. Secret government agents can facilitate secret bulk access to company datacenter information[Daileda 2017]. It is a felony for a citizen or company to reveal secret orders that it has received from the country that has jurisdiction over them or to expose an undercover government agent[Bell 2016; Vincent 2016].

It is fundamental engineering reality that a company's geographically distributed datacenters cannot be *verifiably* audited for the reasons explained here. For resilience, information must be redundantly stored in multiple datacenters meaning that exfiltration could be from any datacenter. In order to detect and prosecute criminal suspects (including alleged terrorists), governments need real-time high-bandwidth access between their security datacenters and the datacenters of their domestically-domiciled companies. There is no effective way to audit that encrypted government traffic out of companies datacenters is not performing mass surveillance. Furthermore, each individual datacenter cannot be verifiably audited (even by the company that owns/operates it) because it runs hundreds of millions of lines of code from multitudinous sources that are continually being updated in real-time. Consequently, it is an practical impossibility to convincingly verify that a foreign-domiciled company is indeed not making it possible for the government that has jurisdiction over it to perform mass surveillance using information from the company's datacenters.

Verifiably ending mass surveillance

Taking note of previous mass surveillance of the its citizens using the equipment and Internet services of foreign companies, the head of Cyberspace Administration of China stated: "It doesn't matter what you (foreign-domiciled companies) say, you should let our internet safety department do a safety assessment. We need to reach our own conclusions to put the consumer at ease."[Timmons 2015]

The US government has blocked the China-domiciled communications company Huawei from operating in the US for fear that the company would create back doors in its equipment that could allow the Chinese military or Beijing-backed hackers to obtain sensitive information. Then NSA hacked Huawei's servers so that when Huawei sold equipment to other countries — including nations that avoid buying American products — the NSA. could secretly operate Huawei's computer and telephone networks to conduct surveillance and potentially, offensive cyberoperations. According to an NSA document obtained by the New York Times, "We (NSA) want to make sure that we know how to exploit these products (to) gain access to networks of interest." [Mozur and Perlez 2016] William Plummer, a senior Huawei executive then based in the United States, said

A foreign-domiciled entity will be prohibited from storing sensitive domestic information in its datacenters except as explicitly enumerated for purposes of domestic law enforcements.

the company had no idea it was an NSA target, adding that in his personal opinion, “The irony is that exactly what they (NSA) are doing to us is what they have always charged that the Chinese are doing through us ... If such espionage has been truly conducted, then it is known that the company [Huawei] is independent and has no unusual ties to any government, and that knowledge should be relayed publicly to put an end to an era of mis- and disinformation (by US).”[Sander and Perlroth 2014] Huawei has subsequently passed independent security reviews against its providing backdoors in its equipment[Thomas 2015]. The precedent by the US government with regards to Huawei provides justification for the Chinese government to take similar measures to protect Chines national security[Timmons 2015; Mozur and Perlez 2016; China National People’s Congress 2016].

For national security reasons, other nations are also demanding that the domestic sensitive information not be accessible in the datacenters of foreign-domiciled corporations[Bot 2015; Castro and McQuinn 2015]. Storing sensitive domestic IoT information (such as from cell phones, bedroom TVs, cars, health prosthetics, and machine tools) in datacenters of foreign-domiciled companies can represent an enormous risk to a nation's national security[Chappell 2017; Disconnect 2015; Farrell and Newman 2016; Herbert 2016; Leyden 2014]. The security threat to a country comes from other countries use of sensitive information including personal information of its citizens, proprietary information of its companies, and its own government information (including military) gathered by foreign-controlled IoT. Because datacenters of foreign-domiciled corporations cannot be verifiably audited, nations will require that companies be domestically domiciled if they store sensitive domestic information in their datacenters. This can be done by requiring that for national security reasons, a foreign-domiciled company that has sensitive domestic information in its datacenters must create a new independent domestically-incorporated company to operate its domestic business. Since the new domestically-incorporated company will be under the jurisdiction of the nation in which it operates, that nation can have greater assurance that the company is not providing sensitive information in its datacenters to foreign governments.

In order not to be forced to domestically re-incorporate in every country, trans-national companies can survive by storing sensitive information in domestic citizen, corporate, and government Islets instead of storing it in their datacenters. In this way, trans-national IoT manufacturers can thrive while realizing the enormous potential benefits of IoT. Furthermore tans-national Internet companies can thrive while still profiting from advertising that is brokered through Islets.

Nothing Is Beyond Our Reach (NIBOR)

According to FBI form Director James Comey: “There is no such thing as absolute privacy in America.” continuing with “Even our memories aren’t private.” [Borger 2017] The thrust of Comey's comments was that no device should be beyond the FBI's reach given a court order, which will include hologlasses (holographic glasses).

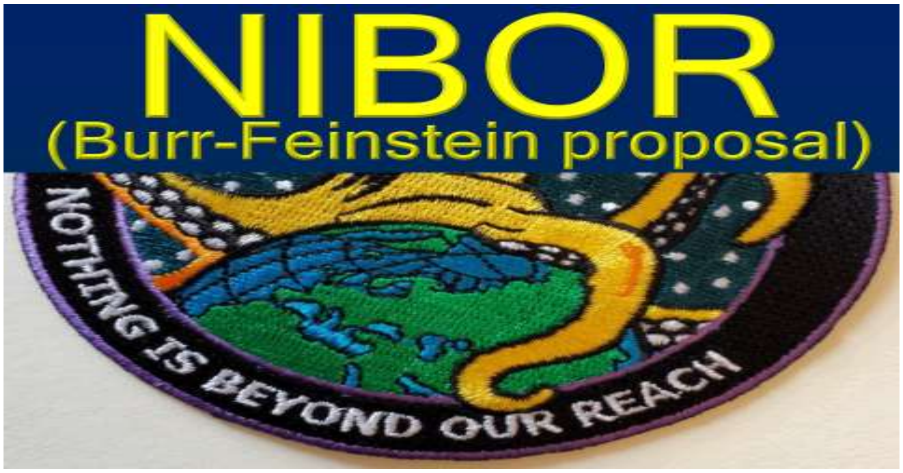
Backdoors in hologlasses could become the greatest threat to civil liberties

Within 10 years, hologlasses are projected to become almost as common as cell phones [Mackie 2016; Mundy 2016]. A backdoor in hologlasses would enable an I-see-and-hear-what-you-see-and-hear

Using Hologlasses in Car Assembly [Erikson 2015] capability that would provide extraordinary insight into what the wearer is thinking.

In order to enable a Nothing is Beyond Our Reach[2] [NIBOR] system. [Burr and Feinstein 2016] proposed the following legislation:

> *"covered entities*[3] must provide unencrypted information and technical assistance[4] to the government pursuant to a court order."[5]



NIBOR is not inexpensive

NIBOR is a further development beyond a CIA proposal[CIA 1996; Rotenberg 2015] in order to implement [Burr and Feinstein 2016], which addresses the following issues identified in [Abelson, *et. al.* 1998]:

- **Keys**: A NIBOR public/private key pair slice is created in a Faraday cage by special hardware in multiple, independent US government command posts in such a way that the private key slice never leaves the Faraday cage in which it was created (except for hardware secured backup). Encryption/decryption is performed in the Faraday cage invisibly to all software of its command post.[6] Public keys are distributed to authorized manufactures for installation in IoT devices.
- **Internet**: In order to connect with the public Internet, a device must present a certificate[7] from the manufacturer that if it receives a packet that decrypts using its public key, then it immediately uses the packet as a bootloader to take over the device without disrupting its ongoing activities using a hard-to-detect virtual machine. In order to operate in the US on the public Internet, a device from abroad (such as a cell phone) must present an import certificate that allows the US government to negotiate with a foreign government about allowed use of the device in the US.
- **Security**: Security risk is mostly assumed by the manufacturers of IoT devices that they cannot be taken over except as described above. If necessary, a device can be taken over repeatedly.
- **Cost**: The multiple command post crypto key security system described above can be used for other national security operations such as securing nuclear weapon keys. It will not be inexpensive to create and operate NIBOR.

[2] "'Nothing is beyond our reach' defines ... the value it[the mission] brings to our nation .." according to a US National Reconnaissance Office spokesperson [Hill 2013]. NIBOR was subsequently adopted for the implementation of the Burr-Feinstein proposal because it is so utterly appropriate.

[3] *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

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

[5] 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).

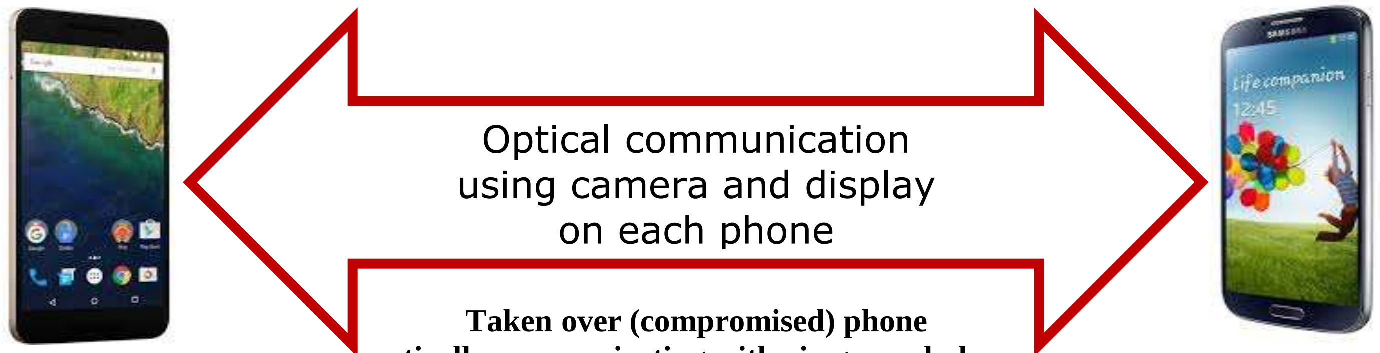
[6] Private keys of command posts can be collectively (n out of m) backed up in other command posts

[7] The certificate can be authenticated using a challenge-response protocol [Yu and Devadas 2017]. Pakistan already requires that mobile phone users must be registered by the government. [Newton 2015]

Unlike distributed corporate datacenters, personal Islets and IoT devices are simple enough that they can be verifiably audited against backdoors[Hewitt 2016b]. For reasons of national security, cyberaudits will increasingly be demanded for imported devices in order to protect sensitive citizen, corporate and government (including military) information[Castro and McQuinn 2015; Timmons 2015; Farrell and Newman 2016]. However, the adoption of mandatory backdoors in each country would make cyberauditing more challenging because of the additional requirement to verify that foreign governments cannot access capabilities installed for a domestic backdoor [Watson 2014].

NIBOR Counter Measures

However, cell phones can easily store and communicate encrypted communication that could not be read by the FBI by using wireless communication to/from medical and other apps (such as in insulin pumps, elderly anti-fall prosthetics, and computer eyewear). Consequently to implement NIBOR, once a cell phone is taken over using a court-authorized backdoor, then any device that network connects to it must also be able to be taken over to help defeat off-line encryption. This means that all Internet-connected medical IoT devices must be able to be taken over lest they be used in offline encryption to defeat NIBOR. NIBOR is a threat to citizens' civil liberty because it makes no allowance for protection against self-incrimination by extremely intimate health devices, and hologlasses. The US judiciary has indefinitely imprisoned a defendant (16 months and counting) for refusing to turn over access of personal IoT devices to the government even though the matter is under appeal.[Jordan, Vanaskie, and Nygaard 2016]



Taken over (compromised) phone optically communicating with air-gapped phone

To protect their sensitive information, citizens can air gap access to Islets using optical communication. For example in the diagram above, a cell phone on the public Internet air-gapped with another cell phone not on the Internet.[8] In this way voice conversations and other communications can take place that cannot be understood by the FBI because encryption/decryption is performed by devices that have not been taken over. Presumably, taken-over devices will attempt to detect that such surreptitious communication is taking place in order to perform overt countermeasures.

Government ordered	Intended effect	Counter measure
operator-compromised devices	operator provides plain-text	open source operating systems not controlled by operator
hardware-enabled backdoor for Internet-connected devices	backdoor provides plain-text	Islets air-gapped from Internet

NIBOR (Nothing Is Beyond Our Reach) Counter Measures

[8] Precautions are needed to ensure that the taken-over cell phone does not intercept other signals, such as speech audio or electro/acoustical from Islet equipment.

Conclusion

> "Our greatest enemy is our own apathy."
> [Mullinax 2011]

Islets can serve two very important functions: protect citizen sensitive information against mass government surveillance and provide a means for IoT manufacturers and Internet companies to thrive instead of risking being destroyed because it cannot be verified that their datacenters are no longer being used for mass surveillance[Bot 2015; Castro and McQuinn 2015; Farrell and Newman 2016; Hewitt and Woods assisted by Spurr; Hobak 2013; Hewitt 2016b].

By not storing sensitive information in datacenters of foreign-domiciled companies, Islets provide means for manufactured IoT to be imported without violating national security. Furthermore, Islets provide a way for trans-national Internet companies to continue to earn advertising revenue -- but without violating citizens' most sensitive information and without violating national security by continuing to share massive amounts of the nation's information with foreign governments in the datacenters of foreign-domiciled companies.

Governments must still be able to detect and prosecute criminal suspects (including alleged "terrorists"). Outside of citizens' Islets protected against self-incrimination, governments will be able to obtain sufficient information for law enforcement by making use of information in datacenters, including all transactions through financial institutions, physical movements outside the home, as well as tracking information from cell towers and connecting to the public Internet.

Acknowledgements

This article has greatly benefited from detailed critiques and organizational suggestions of Alan Karp as well an anonymous highly-experienced professional editor, 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 Whitfield Diffie, Timothy Edgar, Ron Rivest, Marc Rosenberg, and Peter Neumann.

The author's Erlang keynote address covers some of the material in this article [Hewitt 2016a].

The Author

Carl Hewitt is an MIT emeritus professor and Board Chair of the International Society for Inconsistency Robustness (iRobust™).

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

Appendix: Implementation of Islets

In order for Islets to be credible, they must be efficiently and inexpensively implemented as described below. In order to be robust, the implementation of an Islet needs to be distributed across multiple IoT devices including cell phones, personal computers, routers[That, Cerf, et. al. 2015], TVs, refrigerators, cars, and climate control systems. A distributed implementation of an Islet is needed because any of these IoT devices can be taken out of service or become disconnected from other devices without warning.

Islets have large amounts of pervasively inconsistent information because IoT devices are only intermittently connected resulting in delayed coordination and because their sources of information are inconsistent including human input and information from the Web.

Unfortunately, current computer information systems lack fundamental inference capabilities needed by Islets. The two most common approaches, formalization using Classical First Order Logic, and statistical reasoning using machine learning, can fail catastrophically in the face of inconsistent information.

- In classical logic, any possible conclusion logically follows from a (hidden) inconsistency.
- In current “Deep Learning” correlation engines inconsistencies are treated as “noise” that can produce unstable probability assessments washing out the ability to draw reliable conclusions.

Early on, computer scientists began to use mathematical logic to develop theories for Intelligent Applications [McCarthy 1958]. Beginning with Planner [Hewitt 1969], programming languages were developed for automating the use of logic with the aim of developing “micro-theories” of domains of knowledge and then further “between-domain theories” to relate them. Using mathematical logic in in this way did not work out well because:

- There is no practical way to determine if a micro-theory is consistent.
- As a micro-theory becomes larger, it invariably develops (hidden) inconsistencies.
- There are pervasive ineradicable inconsistencies in attempting to relate information in different micro-theories

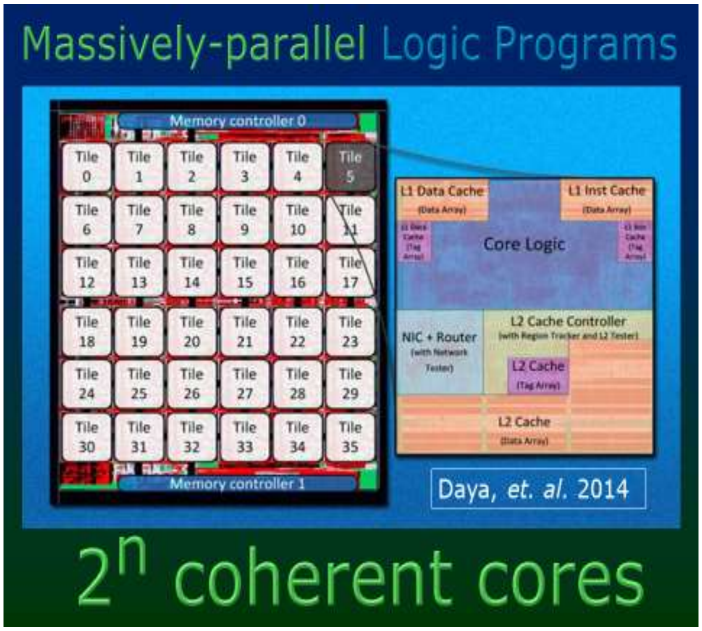
Islets need “Big Ontology” (science and engineering of large information systems of practice), which fundamentally improves on both the classical logic and “Deep Learning” correlations. Big Ontology systems need inconsistency robust reasoning[Hewitt and Woods assisted by Spurr 2015; Meyer 2015] because they have numerous implicit unknown inconsistencies as well as numerous known ones:

- Inconsistencies are ineradicable and can be subtle.
- There is no practical way to test for inconsistency.
- Big Ontology information is meaningful and useful although formally inconsistent.

Inconsistency Robustness needs massive closely-coupled concurrency for its implementation for which the “Actor” abstraction is ideally suited[Hewitt 2015b, 2015c, 2016a] both as a framework for modeling, and as the basis for practical implementations[Bonér 2016; Bernstein, Bykov, Geller, Kliot, and Thelin 2014]. Actors provide modularity and security without imposing any overhead on computation and storage. Existing IoT legacy systems can be extended using Actors without requiring their re-implementation.

Inconsistency Robustness Direct Logic facilitates systems development by removing the requirement that a system must attempt to maintain absolute consistency of its information (as in a relational database). Removing this requirement facilitates massive parallelism in reasoning using coherent many-core computers [Daya, et. al. 2014; Jones 2017]. Logic Programs gain performance through the following:

- massive parallelism in forward/backward inference and ontological inference
- synergy by bringing together processing on assertions, goals, and ontological descriptions.


Massively-parallel Logic Programs

Daya, *et. al.* 2014

2^n coherent cores

The Art of War can be used to illustrate Logic Programs. For example, "Appear strong when weak and appear weak when strong." might be applicable when there is a goal to bluff as expressed in the following Logic Programs:

When goal BluffOpponents[x:Army] **do** (**When goal** Weak[x] **do** setGoal Appear[Strong[x]])[9]
When goal BluffOpponents[x:Army] **do** (**When assertion** Strong[x] **do** setGoal Appear[Weak[x]])[10]

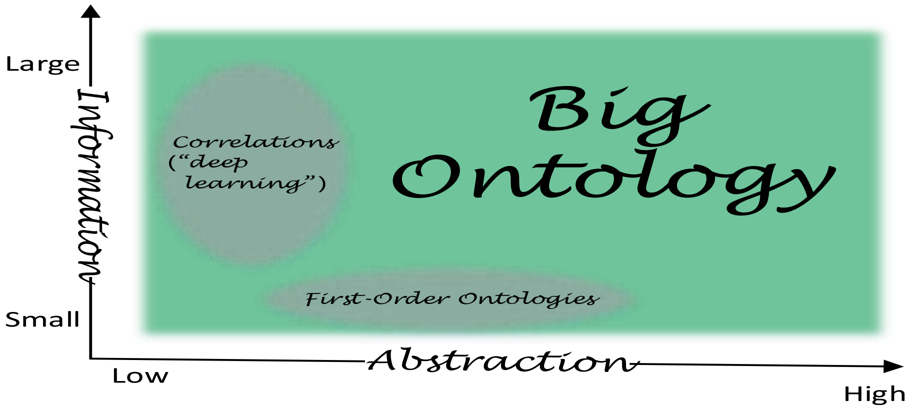
To facilitate inconsistency robustness, Logic Programs can provide both fine-grained control over both forward and backward inference as illustrated below:

- Forward inference
  - **When assertion** Strong[x**:**Army] **do** assert **not** Weak[x][11]
  - **When assertion** Weak[x**:**Army] **do** assert **not** Strong[x][12]
- Backward inference
  - **When goal** Weak[x**:**Army] **do** setGoal **not** Strong[x][13]
  - **When goal** Strong[x**:**Army] **do** setGoal **not** Weak[x][14]

Logic Programs must be robust against inconsistencies. For example, the common situation of having multiple simultaneous goals (e.g. to both bluff opponents and to intimidate them) often leads to conflict, e.g., adding the following logic program to the ones above:

When goal IntimidateOpponents[x**:**Army] **do** setGoal Appear[Strong[x]][15]

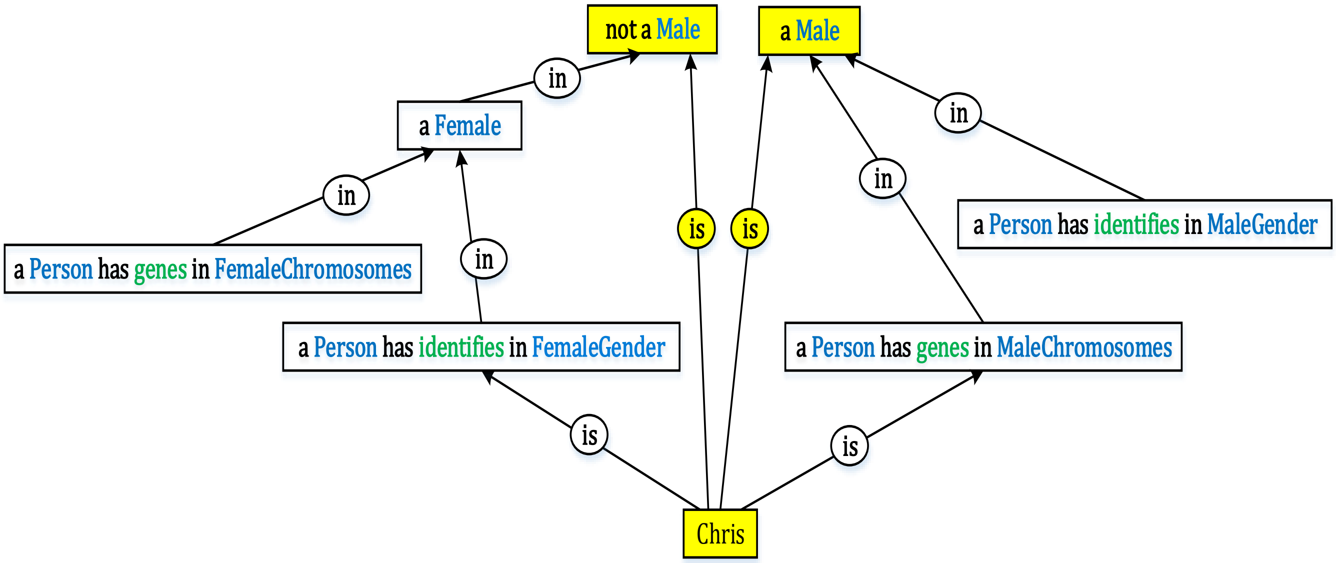
Ontological information is crucially important:



Big Ontology is Future of Big Info and Analytics

[9] When goal to bluff opponents, then when weak, set goal to appear strong.
[10] When goal to bluff opponents, then when strong, set goal to appear weak.
[11] When asserted that x is strong, assert that x is not weak.
[12] When asserted that x is weak, assert that x is not strong.
[13] When goal that x is a strong, set subgoal that x is not weak.
[14] When goal that x is a weak, set subgoal that x is not strong.
[15] When goal to intimidate the enemy, set subgoal to appear strong.

Inconsistencies commonly arise in large ontologies. For example, the following can arise in the case of a transgender person in which disentangling maleness can be very problematical in medical/social contexts[16]


not a Male
a Male
in
a Female
in
in
in
a Person has identifies in MaleGender
is
is
in
a Person has genes in FemaleChromosomes
a Person has identifies in FemaleGender
a Person has genes in MaleChromosomes
is
is
Chris

Chris is both a Male and not a Male depending on circumstances

The above illustrate the following points about Big Info and Analytics:

- Inconsistencies are pervasive and ineradicable in large information systems requiring the use of inconsistency robust reasoning [Hewitt and Woods assisted by Spurr 2015] because it is unsafe to use first-order logic for possibly inconsistent information.
- Inconsistency robustness facilitates theory (ontology) development because (unlike in first-order logic) a single inconsistency is not disastrous.
- Big Ontologies can incorporate correlations and other statistical information
- Even though information is often inconsistent, it is not thereby made meaningless and can still be coherent. [Law 2004]

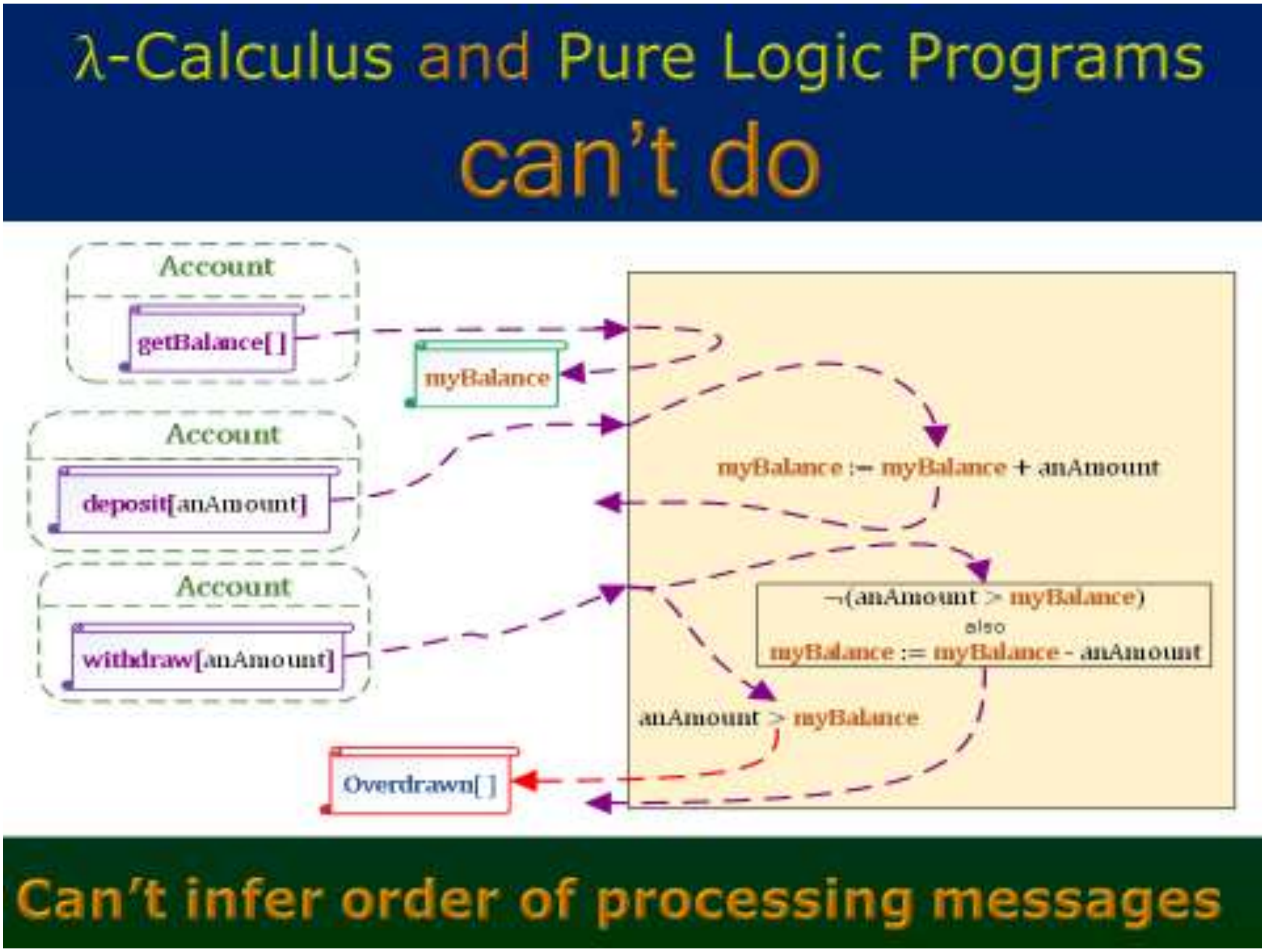
Actors employ message passing using strong types as a fundamental unit of communication because of semantic integrity that is important in IoT operations. Using messages as the architectural unit of communication is a fundamental advance over existing IoT Internet protocols. Existing IoT communication systems are architected on the basis of packets which can be organized into to byte streams. However, neither packets nor byte streams are themselves semantically meaningful. Consequently, additional layers of software in current systems must be layered (and then parsed) on top of byte streams to create meaningful messages. Instead, messages should be foundational to network communication and sent encrypted.

Each IoT device should have public keys whose corresponding private keys are hardware protected and never revealed to software on the device. Furthermore, each IoT device should have a hardware-protected public key of its current owner. Actors support for the integration of coordination and action across multiple IoT devices with strong types using

[16] e.g., surgery, hormones, dress, pronouns, etc.

cryptography[Hewitt 2015a]. In this way cryptography can be naturally integrated into the programs of applications running on multiple IoT without requiring that application programs manage encryption keys[Hewitt 2015a, 2015b].

The Actor Model is much more powerful than nondeterministic Turing Machine and lambda calculus models of computation. For example, the Actor diagrammed below cannot be implemented using a nondeterministic Turing Machine or by using the Lambda Calculus because both models of computation leave out the communication capabilities required for its implementation.



λ-Calculus and Pure Logic Programs can't do

Can't infer order of processing messages

What Nondeterministic Turing Machines, Parallel Lambda Calculus, and Pure Logic Programs *can't* do[Hewitt 2015a]

The above diagram is for the implementation of an Actor of type SimpleAccount with variable myBalance, which behaves as follows:

- If an **availableBalance[ ]** message is received, then return **myBalance**.
- If a **deposit[**anAmount**]** message is received, then increment **myBalance** by anAmount and return.

- If a **withdraw[**anAmount**]** message is received, then if anAmount>**myBalance** then decrement **myBalance** by anAmount and return, else throw an **Overdrawn[ ]** exception.

Strong types enable application programs to use encryption automatically with requiring application programs to include encryption/decryption operations and manage encryption keys.

Use of passwords is an enormous threat to the security of IoT devices. Consequently, they must be eliminated in favor of biometric authentication linked to verifiable public keys. Each citizen and organization needs public keys that can be verified using multiple independent online directories, preferably maintained in multiple countries that are difficult to coerce.

Actors are extremely well suited for implementing the massive concurrency required for Islet inconsistency-robust applications that Islets require. IoT Islet devices need to coordinate in terms of high-level assertions and goals in addition to currently used lower-level imperative messages (such as **availableBalance**, **deposit**, and **withdraw** illustrated above). Using Actors, the hardware cyberdefenses described below can make it dramatically more difficult to find and exploit security vulnerabilities in Islets. For example, Faraday cages can be constructed in a processor package so encryption/decryption can be performed without the possibility of inadvertent emanations that could be measured or exploited, because all external communication to a cage would be through optical fiber and the cage's power supply is filtered. This way, encryption keys and encryption/decryption processes are protected against inadvertent emanations. In such a Faraday cage, advanced cryptography (such as NTRU Prime[Bernstein, Chuengsatiansup, Lange and Vredendaal 2016]) cannot be feasibly attacked through any known method, including quantum computing.

Hardware can likewise help protect software in Islets, including operating systems and applications. For example, all traffic between a processor package and RAM can be encrypted using a Faraday cage to protect a potentially targeted app (which is technically a process) from operating systems and hypervisors, other apps, and other equipment, including baseband processors, disk controllers, and USB controllers. Even a cyberattack that compromises an entire operating system or hypervisor would permit only denial of service to its applications and not give access to any application or related data storage.

Similarly, every-word-tagged processors can be used to protect each Islet Linux kernel object and each Java object in an app from other such objects by using a tag on each word of memory that controls how memory can be used. Tagged memory can make it much more difficult for a cyberattacker to find and exploit software vulnerabilities, because compromising a Linux kernel object or a Java application object does not automatically give power over any other object.

Such individual processor-package cyberdefense methods and technologies will make it possible, within, say, the next five years, to construct a highly secure board with more than 10^3 coherent cores with each core more powerful than any currently available core and with 10^{-8} second average core-to-core latency (compared to often greater than 10^{-4} second latencies for marshaled messages between Linux processes) that can produce over 10^{13} operations per second Such equipment will provide the power needed to implement the Inconsistency Robust applications that will be needed to make Islets effective[Hewitt and Woods assisted by Spurr 2015; Hewitt 2016a].

References

Hal Abelson, Ross Anderson, Steven Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter Neumann, Ronald Rivest, Jeffrey Schiller, and Bruce Schneier. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* Schneier on Security. 1998.

Anushka Asthana *British councils used Regulation of Investigatory Powers Act to secretly spy on public* Guardian. December 25, 2016.

Laurel Beeler, US Magistrate Judge. *In the Matter of the Search of Content that is Stored at Premises Controlled by Google* Case No. 16-mc-80263-LB. April 17, 2017.

Ron Bell, General Counsel, Yahoo. *Letter to James Clapper, DNI, US ODNI* October 19, 2016.

Julian Borger. *FBI's James Comey: 'There is no such thing as absolute privacy in America'* Guardian. March 8, 2017.

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

Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange and Christine van Vredendaal. *NTRU Prime* Cryptology ePrint Archive. Report 2016/461. May 11, 2016.

Philip A. Bernstein, Sergey Bykov, Alan Geller, Gabriel Kliot, and Jorgen Thelin. *Orleans: Distributed Virtual Actors for Programmability and Scalabilit*y Microsoft MSR-TR-2014-41. March 24, 2014.

Jonas Bonér. *Preface.* in "Reactive Messaging Patterns with the Actor Model" by Vaughn Vernon. Addison-Wesley. 2016.

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

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

Michael Capuano. *TVs spying on us is just the tip of the iceberg. Is Congress ready to act?* Guardian. March 9, 2017.

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.

Bill Chappell. *Banned In Germany: Kids' Doll Is Labeled An Espionage Device* NPR. February 17, 2017.

CIA (US Central Intelligence Agency). *Memo for the Vice President* September 11, 1996.

China National People's Congress. *2016 Cybersecurity Law.* China Law Translate. November 7. 2016.

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

Scott Erikson. *Microsoft HoloLens and Volvo Cars explore the future of car buying* Microsoft. November 19, 2015.

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.

Colin Daileda. *D.C. police demand Facebook hand over data on Trump protesters* Mashable. February 7, 2017.

Bhavya Daya, Chia-Hsin Owen Chen, Suvinay Subramanian, Woo-Cheol Kwon, Sunghyun Park, Tushar Krishna, Jim Holt, Anantha Chandrakasan, and Li-Shiuan Peh, *SCORPIO: A 36-Core Research Chip Demonstrating Snoopy Coherence on a Scalable Mesh Network-on-Chip with In-Network Ordering* ISC-2014.

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

European Court of Justice. *Judgment of the Court* December 21, 2016.

William Enck, et. al. *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones* OSDI'10. October 2010.

Henry Farrell and Abraham Newman. *The Transatlantic Data War: Europe Fights Back Against the NSA.* Foreign Affairs. January/February 2016.

Shanika Gunaratna. *Amazon's Echo Look debuts, prompting storm of privacy concerns* CBS News. April 27, 2017.

Louis Hansen. *Another approach to autonomous vehicles – slow and steady* SiliconValley.com. Jan. 27, 2017.

David Herbert. *This Company Has Built a Profile on Every American Adult*. Bloomberg Businessweek. August 5, 2016.

Kashmir Hill. *U.S. Spy Rocket Has Octopus-Themed 'Nothing Is Beyond Our Reach' Logo. Seriously.* Forbes. December 5, 2013.

Carl Hewitt. *Planner: A Language for Proving Theorems in Robots* IJCAI. 1969.

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

Carl Hewitt. 2015a. *Actor Model of Computation for Scalable Robust Information Systems* in Inconsistency Robustness. College Publications. 2015.

Carl Hewitt. 2015b. *ActorScript™ extension of C#®, Java®, Objective C®, C++, JavaScript®, and SystemVerilog using iAdaptive™ concurrency for antiCloud™ privacy and security* in Inconsistency Robustness. College Publications. 2015.

Carl Hewitt. 2015c. *Inconsistency Robustness in Logic Programs* in Inconsistency Robustness. College Publications. 2015.

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

Carl Hewitt.2016a. *Actors for CyberThings.* Erlang Keynote. YouTube. March 23, 2015.

Carl Hewitt. 2016b. *Security Without IoT Mandatory Backdoors: Using Distributed Encrypted Public Recording to Catch & Prosecute Suspects* Social Science Research Network. 2795682. June 16, 2016.

Cullen Hobak. *Terms and Conditions May Apply.* Phase 4 Films. 2013.

Jordan, Vanaskie, and Nygaard. *USA v. Apple Macpro Computer Apple Ma* District Case Number: 2-15-mj-00850-001. 2016.

John Ioannidis. *Why Most Published Research Findings Are False* PLoS Medicine. 2(8): e124. 2005.

Marsi Kendall. *Uber pulls self-driving cars from San Francisco streets, bowing to regulators' demands* Mercury News. December 21, 2016.

John Law. *After Method: mess in social science research* Routledge. 2004.

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

John Leyden. *Hey, does your Smart TV have a mic? Enjoy your surveillance, bro.* The Register. May 10, 2014.

Ewen MacAskill. *'Extreme surveillance' becomes UK law with barely a whimper* Guardian. November 19, 2016.

James Mackie. *ODG 4K Augmented Reality Review, better than HoloLens?* YouTube. Dec 20, 2016

Antonio Garcia Martinez. *Chaos Monkeys: Obscene Fortune and Random Failure in Silicon Valley* Harper 2016.

John McCarthy. *Programs with common sense* Symposium on Mechanization of Thought Processes. National Physical Laboratory. Teddington, England. 1958.

Joseph Menn. *Yahoo secretly scanned customer emails for US intelligence* Reuters. October 4, 2016.

JJ Meyer. *Review of Inconsistency Robustness.* College Publications. 2015. http://collegepublications.co.uk/review/lgc00030.pdf

Annemarie Mol. *The Body Multiple: ontology in medical practice* Duke University Press. 2002

Chris Monroe. *Amazon agrees to share Echo data with Arkansas prosecutor in murder case* CBS News. March 7, 2017.

Walt Mossberg. *Why does Siri seem so dumb?* The Verge. October 12, 2016.

Paul Mozur and Jane Perlez. *China Quietly Targets U.S. Tech Companies in Security Reviews* New York Times. May 16, 2016.

Bill Mullinax *Our Greatest Enemy* Outword Magazine. May 22, 2011.

Jon Mundy. *Microsoft CEO reckons HoloLens will be 'the ultimate computer'* Trusted Reviews. August 4, 2016.

Jennifer Newton. *EVERY mobile phone user is ordered to have their fingerprints taken in Pakistan as part of country's new anti-terror laws* DailyMail.com February 26, 2015.

Dan Packel. *Pa. Judge Says Google Must Turn Over Foreign Server Data* Law360. February 6, 2017.

Abby Philip. *A paralyzed woman flew an F-35 fighter jet in a simulator — using only her mind.* Washington Post. March 3, 2015.

Marc Rotenberg. *EPIC: The First Twenty Years* in "Privacy in the Modern Age" The New Press. 2015.

David Sander and Nicole Perlroth. *N.S.A. Breached Chinese Servers Seen as Security Threat* New York Times. March 22, 2014.

Matt Shore. *Chips with Everything* The Guardian. January 7, 2017.

Rich Tehrani. *AirHopper: Even Air-Gap Networks are Not Secure* Tehrani Communications and Technology Blog. November 20, 2014.

Dave That, Vint Cerf, et. al. *Request for the Allowance of Optional Electronic Labeling for Wireless Devices* Letter to US FCC. RM11673. 2015.

Sam Thielman. *Your private medical data is for sale – and it's driving a business worth billions* Guardian. January 10, 2017.

Daniel Thomas. *Huawei does not pose risk to UK national security, report finds.* Financial Times. March 31, 2015.

Meng-Day (Mandel) Yu and Srinivas Devadas. *Pervasive, Dynamic Authentication of Physical Items* CACM. April 2017.

Heather Timmons. *Apple is reportedly giving the Chinese government access to its devices for "security checks"* Quartz. January 23, 2015.

James Vincent. *The UK is about to wield unprecedented surveillance powers — here's what it means* The Verge. November 23, 2016.

Steve Watson. *Intel CEO refuses to answer questions on whether NSA can access processors* Infowars. February 20, 2014.