Going Bright: How the Internet of Things Could Revolutionize Intelligence Collection and Analysis

AUGUST 2016

2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

ACKNOWLEDGEMENTS

We would like to first thank the Office of the Director of National Intelligence (ODNI) for its generous funding and support for our study and learning journey to Silicon Valley. We are also very grateful to the Department of Homeland Security (DHS) for its support during the duration of the program.

We could not have completed this study without the unwavering support and dedication of Mr. Richard ("Rick") Harris of the Office of Cybersecurity and Communications, DHS our devoted Team Champion who steered us throughout this study and helped turn an idea into a product.

We would like to acknowledge and thank each member of our public-private sector working group for their tireless efforts from around the U.S. which includes Krystle Kaul, Robert Knight, Garrett McNamara, Ian Mitch, Casey Moles, Pinar Moore, Thomas Saly and Kenneth Stavinoha. We would like to highlight the tremendous contributions of Ms. Kaul in identifying and liaising with smart cities experts in addition to planning and coordinating the group's "Learning Journey" to Silicon Valley, and the detailed work of Mr. Mitch in compiling and organizing this paper and accompanying infographic.

We are very thankful for all the unique insight we received from interviewees who contributed to this report by educating our group on the many aspects of the Internet of Things, and we take full responsibility for any and all errors of fact or interpretation implied or explicit in this paper. Our interviewees include the Internet of Things (IoT) Village sponsors at DEF CON as well as federal and commercial practitioners from Silicon Valley and Washington D.C. We are thankful for the interesting and diverse perspectives particularly from: Mr. Gary Haslip, Deputy Director, Chief Information Security Officer (CISO) - City of San Diego; Mr. Ted Harrington, Executive Partner at Independent Security Evaluators; Mr. Dan Miesseler, Practice Director, Client Advisory Services; Mr. Lyon Yang, Security Engineer; Mr. Brian Knopf, Chief Security Researcher at oneID; Mr. Mark Stanislav, Manager, Security Advisory Services at Rapid7; Mr. Wesley Wineberg, Senior Security Software Engineer, Azure Red Team at Microsoft; Mr. Craig Young, VERT Security Researcher at Tripwire; Mr. Peter Hirshberg, CEO Re:imagine Group; Dr. Tim Campbell, Chairman, Urban Age Institute and Global Fellow, Woodrow Wilson International Center for Scholars; Ms. Elecia White, Embedded Systems Consultant, Logical Elegance; Mr. Jay Nath, Chief Innovation Officer (CIO) to the Mayor of San Francisco; Mr. William Barkis, the Internet of Things Advisor to CIO of San Francisco (SF); Ms. Kathleen Clark, Social Media Manager & Digital Communications Strategist at the Department of Technology; Mr. Param Singh, CEO at IoTracks Inc. and Advisor to the CIO of SF; Ms. Melanie Nutter, Sustainability Executive and head of Nutter Consulting; Mr. Kurt Buecheler, Senior Vice President of Streetline; Dr. Peter Williams, Chief Technology Officer of "Big Green Innovations" at IBM; Mr. Vishi Iyer, IBM Security, Global Cloud & IoT Security Strategy Leader; Mr. Michael Liebhold, Distinguished Fellow, Institute for the Future; Dr. Brian Bartholomeusz, Executive Director of Innovation Transfer, Stanford University; Mr. Shaun Kirby, Chief Technology Officer of Cisco Consulting Services; Mr. Irfan Saif, Advisory Principal, Deloitte & Touche LLP; Dr. Eric Paulos, Assistant Professor of Electrical Engineering and Computer Sciences at UC Berkeley; Dr. Anthony Joseph, Chancellor's Professor at UC Berkeley; Dr. Anthony Townsend, Principal Consultant Bits and Atoms LLC and Smart Cities Expert; Mr. Gordon Feller, Director and Consultant at Cisco Systems; Mr. Rick Hutley, Program Director, Clinical Professor of Analytics at University of the Pacific and Former Vice President of Internet of Everything at Cisco Systems. We are very grateful for their time and valuable perspectives on our study topic.

EXECUTIVE SUMMARY

Going Bright: How the Internet of Things Could Revolutionize Intelligence Collection and Analysis

Over the next decade, advancements in technology could dramatically reshape how US intelligence and law enforcement agencies collect and analyze information to safeguard the American people. The increasing prevalence of Internet connected devices, often referred to as the Internet of Things (IoT), may enable what some describe as the "golden age of surveillance."[1]

Consider, for example, the potential intelligence and law enforcement value of voice-activated household devices—such as Google Home or the Amazon Echo—that listen in on the private communications of its users. Data from autonomous cars might enable real-time tracking of terrorists or could help quickly identify a child abductor. Wearable technologies and activity trackers used by foreign militaries could provide information to US war-fighters on the health, vulnerabilities, and movement of armies.

It is not hard to imagine how the proliferation of Internet connected technologies could enhance the government's ability to detect and disrupt threats. However, our examination of the potential trajectory of the IoT landscape, informed by over thirty interviews with leading IoT experts in academia, government, and the private sector, reveals several potential challenges that are likely to hinder the government's ability to collect and analyze this data.

First, the IC is likely to encounter a variety of legal and technical challenges that will inhibit its ability to access valuable data on threats, particularly inside the US. Increasing privacy and security concerns are driving technology companies to constantly enhance security architectures, which suggests the IC will be tested to keep up with improving encryption standards. Moreover, many companies are promoting data management policies and architectures that seek to prevent governments from accessing this data even when legal means (e.g., a warrant) are used.

We observed this phenomenon most recently with the proliferation of end-to-end encryption in communication platforms as well as with improved default encryption of mobile devices such as the Apple iPhone. Some companies are so determined to prevent the government from accessing their data that they are deleting it before a warrant can even be served.[2] While we do not anticipate all technology companies will go to these lengths to protect their data—and huge volumes of metadata will probably remain unencrypted and accessible to the government—it is likely that valuable data from the IoT will remain outside of the IC's reach.

Additionally, we expect an internet-connected ecosystem will be adopted more rapidly in the United States and slower in countries that are top IC targets. This disparity suggests IoT could present a greater opportunity for our adversary's intelligence services than our own. Consider, for example, the popularity of wearable technologies—such as smart watches and fitness bands—in the United States. Nearly one in five Americans owns a wearable device, including President Obama. The accumulation of data from these devices and the correlation of this information with other behavioral and environmental data create significant counter-intelligence and protection challenges.[3]

Finally, government will likely struggle to effectively analyze large amounts of data collected from IoT devices without greater investment in advanced analytic technologies and data scientists. The advent of IoT could potentially force a dramatic shift in how the intelligence community conducts analysis. Instead of relying primarily on human sources or electronic intercepts to collect single data points, agencies must develop the capability to sift through huge amounts of data to uncover trends and identify threats. However, the government's historical challenges adapting to advancements in technology portend a difficult road ahead in big data analytics. This challenge becomes more acute when considering the government will be in direct competition with big data companies recruiting for talent particularly in Silicon Valley.

We outline below three broad recommendations we believe will better position the intelligence and law enforcement communities to overcome these challenges and realize the opportunities presented by an increasingly connected environment. Most importantly, we believe that forging greater partnerships with companies that are developing and implementing IoT technology holds the greatest potential of improving both the security of these networks and enabling the government to access information it needs to keep America safe. The efforts of technology companies to protect the privacy of their customers through improved encryption is not necessarily incompatible with the government's interests in protecting America from national security or criminal threats. A mutual concern over security should provide some common ground upon which government and companies leveraging IoT technology can work together to secure these networks for the benefit of everyone. Additionally, closer ties between these two communities will likely open the door to greater exchanges of knowledge that might help the government overcome the technology gap it is likely to encounter in the years ahead.

- **Build Trust by Pulling Back the Curtain on Intelligence Activities at Home**. Distrust of the intelligence community among technology companies is primarily rooted in the impression that the government collects digital information on Americans illegally. Indeed, during our discussions in Silicon Valley it was clear that many of the Snowden revelations continue to make industry suspicious of government motives. Intelligence agencies need to begin to chip away at this bias by engaging these communities in public and private forums to better explain their authorities to collect information inside and outside the United States. The IC should also declassify more examples that show how nefarious actors are benefiting from improvements in encryption promoted by some technology companies. Intelligence agencies too often hide behind a curtain of secrecy and a 'need to know' culture that is driving a wedge between it and the communities it seeks to protect. It is time to shift this culture and start to build bridges with those communities, which in the long-run could lead to greater sharing of information that will help the IC better protect America.

- **Move Beyond Transactional Relationships and Help Secure the Internet of Things.** The current relationship between the US government and Silicon Valley is primarily transactional. Typically, the FBI will engage with these companies when it has obtained a court order and requests information on an individual it is investigating. However, strong relationships are a two-way street. The growing threat posed by an increasingly internet-connected environment provides more avenues for these communities to help protect Americans. The IC should promote greater exchanges of information on nefarious actors that seek to exploit connected networks. It should also promote joint-duty assignments that allow IC officers and technology employees to complete rotational assignments in each other's offices. The National Institute of Standards and Technology is exploring the IoT to better understand its impact on both the public and private sectors. Organizations such as the Internet Society and its Internet Engineering Task Force seek to understand and generate IoT standards. The IC should play a role in these efforts and provide briefings to industry informing them of threats.

- **Create ODNI Mission Manager for the Internet of Things.** Collection and analysis of IoT data has the potential to support every IC mission priority that includes terrorism, weapons proliferation and cyber threats. It will require a transition in how strategic analysts write intelligence products relying more heavily on deriving trends from huge amounts of data. Additionally, this shift will require large investments in big data analytic capabilities and scientists capable of sifting through terabytes of information to identify bad actors. Furthermore, it will require coordinating and harnessing the capabilities of all seventeen intelligence agencies preparing for these revolutionary changes. An ODNI mission manager for the Internet of Things would ensure the IC is positioned to keep pace with these evolutions, promote best practices and limit redundancies between agencies.

Going Bright: How the Internet of Things Could Revolutionize Intelligence Collection and Analysis

What is the Internet of Things and How Can the IC Leverage it?

The Internet of Things (IoT) is an abstract concept. Cisco describes it as "a network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data."[4] These devices are connected to the Internet so they can send and receive data both through intra- and inter-networks in real-time. Examples of IoT include traditionally connected devices including phones, computers, and watches along with nontraditional objects such as parking spaces, traffic lights, refrigerators, and garage doors.

Networked devices within a system make it smarter and enable companies and customers to better track transaction activities, collect, collate and analyze information to make better decisions, improve efficiency, and increase productivity. For example, cities are integrating sensors into public transportation systems to collect information that will allow them to reduce traffic flows and adjust routes based on demand shifts.[5] Oil companies are fitting rigs with sensors to better monitor the health and behavior of critical machinery so that they can avoid unexpected downtimes or catastrophic accidents. Refrigerator sensors are being programmed to automatically order groceries when quantities run low.

The technology advancements represented in the IoT could have profound effects on how the IC conducts its business. For decades, US intelligence agencies possessed a virtually unrivalled ability to collect information on its adversaries whether by placing a human source within a targeted organization or by compromising an adversary's computer. Now, every Internet connected device is a potential intelligence collector that could provide more timely, accurate and intimate knowledge of top intelligence targets than traditional collection methods. At the same time, virtually every connected device generates information that may be of equal importance to our adversaries.

Given the amount of personal information networked devices will collect, primarily for commercial uses, the most immediate potential benefit for the IC is an improved ability to conduct surveillance (See attached Infographic). Devices such as in-home security cameras or listening devices, for instance, might provide the FBI with a greater understanding of a suspected terrorist's attack plans (if that information were made available to the IC). In addition, mobile-controlled thermostats and remote-access room lighting can produce pattern of life data inside a residence that would assist law enforcement or intelligence agencies to predict behavior. Autonomous cars, for example, might improve the CIA's ability to spot and assess potential sources based on their daily activities and locations. Fitness monitors might provide political analysts greater insight into foreign leaders' health and wellness habits that might indicate recruitment vulnerabilities or predict health-related leadership changes in that country.

If the IC improves its ability to aggregate multiple data points from IoT devices it will be better positioned to incorporate this information into strategic assessments to help US leaders better understand shifting political, economic, and military trends. Additionally, the IC can help US law enforcement agencies predict and prevent terrorist attacks. For example, the collection of data from wearable technologies used by foreign armies or terrorist groups—data from potentially thousands of individual devices—might provide insights into their location and specialized training that portend new missions. Industrial devices used to manage oil wells and refineries could help better predict fluctuations in gas prices. Data on traffic patterns in smart cities might show when public protests are ramping up, suggesting growing public discontent or indicate the beginning of a coup de 'tat.

While these examples suggest connected devices will provide new methods of collecting and analyzing intelligence, the IoT may also improve the accuracy and timeliness of this information. For example, much of the IoT data will be collected and transmitted in real-time. Compare that to intelligence collected from human

sources that might not have an opportunity to meet with their handler for days or weeks. IoT data can also be more accurate. Information from human sources is often provided second or third hand, while IoT data is collected directly from the source of the device. Finally, data derived from connected devices also has the potential to free-up resources that can be dedicated to other intelligence missions. For example, FBI agents conducting around-the-clock monitoring of a terrorist suspect might require dozens of agents. But, if wearable technologies and devices in smart homes can supplant some of the work of these agents, the FBI can dedicate these resources elsewhere.

Variations in IoT Implementation: Opportunities and Challenges

The IC and law enforcement agencies must consider significant variations in the pace and purpose of IoT implementation, especially in smart cities, to understand the potential opportunities and challenges for collection and analysis. San Francisco and Hong Kong have plans to become "smart cities" by employing IoT technology, as do many other rural and urban entities, but each of these cities will apply IoT for different reasons and objectives. They will likely encounter common challenges using these technologies, such as the need to first integrate and then phase out legacy systems; the need to apply varying legal and governance frameworks; and the need to shape and respond to attitudes and expectations of their communities who must adapt to life in a smart city.

San Francisco and Hong Kong are implementing IoT to alleviate traditional urban problems such as traffic congestion and public safety. They seek to improve government decision-making and responsiveness, and increasing infrastructure reliability and resilience. San Francisco emphasizes the "green" benefits of the IoT and orients its IoT planning on making life better for its citizens.[6] Hong Kong has similar aspirations. IoT technology mitigates urban problems by helping government and citizens to better understand their environments through ubiquitous sensors, big data collection and analytics, and rapid decision-making.

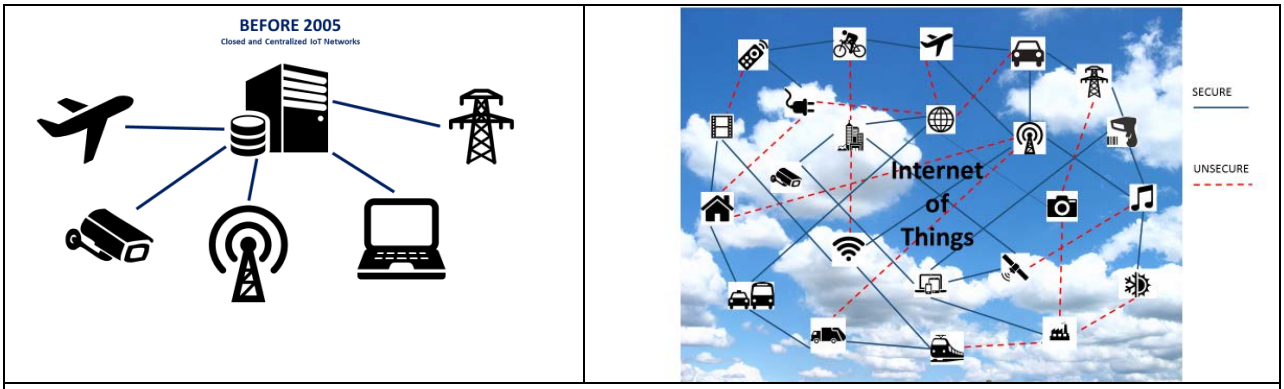
San Francisco and Hong Kong cannot implement IoT from a clean slate and must deal with legacy traffic, infrastructure, power, information management, and organizational structures. How these cities and others deal with legacy issues will likely affect the pace and scale of IoT implementation and in the potential success of IoT initiatives. San Francisco will be conducting pilots to introduce and test IoT applications.[7] Hong Kong can be expected to do the same. This suggests that instrumentation and the resulting data will be much more prevalent in areas where pilot projects occur. In these areas it is likely that legacy technology and infrastructure will be retrofitted or otherwise used to create an IoT-enabled network. Closed Captioned TV cameras are an example of how traditional technology can be used more effectively by improving data aggregation and analytics with sophisticated facial recognition and behavioral analysis software.[8]

Aspiring smart cities will also have to deal with legacy people as they implement IoT technology. San Francisco is employing a bottom-up approach to this issue by creating forums for public discourse and input throughout the IoT urban planning and implementation processes. The city government considers voluntary and active public participation as key to a collective and successful IoT vision. Hong Kong, by contrast, is pursuing a more top-down, technocratic approach to IoT implementation. Although both San Francisco and Hong Kong smart city plans are in the early stages, varying levels of transparency and public acceptance will affect the effectiveness of their respective IoT implementation objectives.

San Francisco and Hong Kong leaders will have to make hard choices on prioritization and resource allocation to fully realize their respective IoT visions. The Silicon Valley culture provides San Francisco with a distinct advantage in talent, technology, and an overall desire to expend these resources to protect the environment and improve individual lives. Inclusive and transparent initiatives are likely to convince people to overcome their natural mistrust of government and support the future that the IoT can bring. On the other hand, it is likely that less open and transparent approaches to IoT implementation could hinder an aspiring smart city's ability to realize many of the benefits of IoT.

Implementation of the IoT will likely be uneven abroad and within the US. IoT adoption will be restrained by legacy systems; funding; social acceptance; and other frictions. Similarly, we anticipate security of the data

will be uneven. The IC is likely to have the greatest access to information in foreign spaces where it will have opportunities to conduct traditional and technical espionage in an IoT environment rich with vulnerable IoT devices and information. Collection opportunities increase as the number of devices increases, and potential access points for penetration will grow (see graphic A). With the massive amounts of data generated by these devices, companies are primarily leveraging cloud storage solutions that provide flexible connectivity. Such an ecosystem provides opportunities to collect this data in-transit or at rest, particularly if IoT technology companies don't invest in expensive security solutions such as firewalls, secure tunnels, dedicated protocols, and encryptions.



Graphic A: The proliferation of connections created by the IoT ecosystem will provide new avenues to infiltrate vulnerable networks to extract data.

Security of the devices will also vary greatly. Some technology companies, particularly those providing services that collect highly personal information from customers are likely to prioritize and market highly secure platforms. We expect others will likely lack the technical expertise to fully secure these devices or may prioritize other device features at the expense of security. In conversations with IoT start-ups in Silicon Valley, we frequently heard that while security was important to manufactures, bringing these devices to market was expensive, and the primary means to lower costs was to reduce the computing and physical power needed for security and encryption. These tradeoffs suggest that many smart devices will be delivered to market with pre-existing vulnerabilities and multiple access points enabling data manipulation or data extraction.

In addition, once these devices are delivered to market, securing them will require routine updates and patches. Many companies deploying these products, however, are not technology savvy and are as unlikely—as companies are today—to fully implement security measures. Consider appliance makers, like Whirlpool, which are fitting their refrigerators and stoves with networked sensors. Given the sheer number of companies deploying networked products to market, we anticipate many will fall short in maintaining robust security of their products and this will provide opportunities for intelligence agencies and malicious actors to penetrate these devices.[9]

For these reasons, we expect many (but not all) networked devices will provide the IC opportunities to collect intelligence from smart technologies abroad. This is good news for the intelligence community—until we consider that many of the countries implementing smart technologies over the next decade are not top intelligence targets. For example, Juniper Research ranked the top five smart cities in 2015 as Barcelona, New York, London, Nice, and Singapore.[10] In 2016, the Director of National Intelligence James Clapper identified Russia, China, Iran, North Korea and terrorist groups primarily located in the Middle East as the actors posing the greatest threat to US national security.[11] This suggests the proliferation of IoT devices could make the US more vulnerable as more cities adopt IoT technologies.

Trusting the Internet of Things

Whether one is in San Francisco or Hong Kong (or anywhere else in the world), the proliferation of internet-connected devices in the IoT will dramatically increase the amount of information collected on individuals while they work, shop, drive around town, or stroll on public streets. Much of an IoT network, particularly at its edge, will be insecure, providing the intelligence community new opportunities to collect and analyze data abroad. However, we foresee several challenges that will hamper collection of this data inside the United States, where the government usually depends on companies to produce the information after obtaining a court order or warrant. But private industry is resisting, in large part because it, and its customers, do not trust the government's ability to secure this data. Instead, many of these companies are promoting security architectures that seek to close all "back doors"—including those accessible to the government. We believe this underscores the need for a "trust triad" between government, industry, and citizens that will involve overcoming varying levels of distrust that exist today. However, we are concerned that growing perception among the public of IoT as a potential realization of the "Orwellian state" will significantly complicate both existing and new trust relationships.

Citizens tend to distrust the government's collection of data and want appropriate restrictions and tangible benefit. However, many of these same citizens tolerate–or even enable–data collection by commercial entities to facilitate the use of a product or service with perceived benefit. The broad implementation of IoT in a smart city environment where citizens may not have "opted in" or feel properly informed of the risk versus reward can foster distrust from the outset. Interviews with government, industry, academia, and IoT subject matter experts consistently cited the need for facilitating public trust at the outset through transparency and some level of inclusion in an IoT initiative.

Industry often views data sharing with governments as a one-way path – the government collects data but either does not reciprocate or fails to provide meaningful value in return. Industry regularly collects data from customers – both government and citizens – largely for use in targeted marketing and sales. The potential breadth and depth of rich data could incentivize industry to partner with government on implementation and operation of an IoT smart city initiative. To facilitate the trust triad, industry rules on data collection, handling, and disclosure that are consistent with governmental responsibilities and regulations in these areas need to be established. Additionally, industry needs to demonstrate that IoT products and services are worthy of trust by implementing measurable and verifiable security and privacy policies and practices.

Federal, State and local governments have responsibilities that necessitate the collection of data – especially in the realm of public safety, security and the provision of social services. A perceived lack of transparency in the types and quantity of data collected on citizens along with the protection and disclosure of that data could be an impediment to trust building. The Edward Snowden disclosures increased society's mistrust of government. The recent incident involving the Office of Management and Budget exacerbated this trend and called into question the government's need and ability to collect and handle personal data securely. Pew Research finds that overall trust in the U.S. government is at the lowest level since polls on the topic began in 1958 and, although this isn't specifically related to the collection and handling of data, it infers the potential for a low tolerance level among citizens for perceived trust violations by their government.[12]

The main issue with the acquisition of domestic data available in an IoT environment that would be used for security purposes is over the tradeoff between privacy over security. There is extreme hesitation among the private sector to provide the U.S. government access to data without incurring backlash from the consumer market. The recent access-shutdown of Twitter data underscores this point.[13] The San Francisco Bay area has been historically sensitive on the issues of privacy and civil liberties, so new entrepreneurs as well as the academic community working to further smart technologies there are apprehensive about voluntarily sharing data with government. The U.S. Government is right to increase cooperation in Silicon Valley, with the creation of the Department of Defense's DIUx facility, aiming in part to bridge the cultural gap between private and public sector.[14] But more needs to be done in this area before the trust gap between government and the public becomes too wide to bridge.

Data Analysis: Challenges and Opportunities

We expect the government will struggle to effectively analyze huge amounts of data collected from IoT devices without greater investment in advanced analytic technologies and data scientists. The advent of IoT potentially will force a dramatic shift in how the intelligence community conducts analysis. Instead of relying primarily on human sources or electronic intercepts to collect single data points, agencies must develop the capability to sift through huge amounts of data to uncover trends and identify threats. But the government's historical challenges adapting to advancements in technology portend a difficult road ahead in the area of big data analytics. This challenge becomes more acute when considering that the government will be in direct competition with Silicon Valley and big data companies for scientist capable of such number crunching.

What is more, much of the raw data the IC is likely to collect from IoT devices will exist in different formats that will be difficult to manage or use. Thus, the IC will need to create analytic methods and technologies to meaningfully categorize and organize the raw data. Furthermore, automating these analytic methods would be most beneficial to the IC due to the substantial amount of data likely to be generated. The IC will need to come up with a data normalization scheme and significantly increase its quality and the capacity of its technology.

Another challenge the IC will likely face is analyzing data in real-time or at least fast enough to inform operational decision-making. The IC's ability to analyze data in real-time depends on several factors including timely access to the data, type of data (video, audio, or text), the timeliness of data normalization (automated or not), number of dedicated data scientists and analysts and availability of other analytical tools. However, the potential benefit of real-time IoT data analysis is enormous potentially for tracking a domestic terrorist's actions in near real-time including location and travel patterns.

Historical IoT data analysis also has advantages. The benefit of historical data is that it can be aggregated and potentially show a pattern-of-life of terrorists and their past activities. This same data can also possibly identify new patterns of activity that might provide indications of other malicious activity. Essentially, the historical data could be used to compare with real-time IoT data.

In the digital world the veracity of analytic conclusions may continue to be constrained by the lack of relevant and timely data; however the overall availability of more and richer data expected in the IoT; the application of increasingly sophisticated analytic algorithms applied against vast stores of data; and the automation of analytics through high speed computing techniques and hardware could improve the intelligence communities' ability to understand terrorist behavior and the political, military, economic and social environments in which they operate. Storing increasingly large and varied amounts of IoT generated data is feasible as suggested by Kryder's law, particularly leveraging cloud storage however, the primary challenge IoT presents to intelligence analysis is the ability to manage (access, process, secure and analyze) that data quickly and make it actionable.[15]

Hong Kong is a hotspot for data storage. In places where this is the case, there exists an opportunity for discreet transmission of data both inbound and outbound internationally. It is not unusual for large organizations to want data replicated across large regions of the globe via hotspots such as Hong Kong, nor would it be unusual for there to be a large amount of data shuffling between these locations. Content distribution network (CDN) companies such as Akamai for example offer this as a service in order to reduce network latency for all of a customer's constituents worldwide. Coupled with adequate encryption and obfuscation data could be transferred to and from Hong Kong to other locations internationally without arousing suspicion. Furthermore, global replication avoids disclosing the consumer of the data because a copy of the data is downloaded from the nearest replication point, in effect using the CDN as an indirect transmission channel to avoid point-to-point communication.

IoT literature abounds with information about architecture, processing and use cases, but not many people in the commercial realm seem to be worried about the ability to store and access increasingly large amounts of

data. Generally, data storage will be distributed across the IoT architecture and into the cloud in a tiered fashion where combinations of processing power, energy, and accumulated data are needed to implement some function such as power distribution in an electrical grid. It is useful to think about IoT data storage as a dynamic process instead of series of traditional and static data farms, particularly when considering the dynamic environments in which intelligence collection and analysis will take place. Francis deCosta identifies three classes of IoT functionality that are useful for expanding the traditional view of data in the IoT in his "Rethinking the Internet of Things."[16] These three classes include end devices at the edges of IoT networks; propagator nodes which aggregate data from end point devices and potentially other propagator nodes, and serve as gateways to the Internet; and integrator functions where analysis and control occur and possibly where humans interface with the IoT network.

As data is transmitted through the IoT from end devices (sensors) to propagator nodes (data aggregation points), and increasingly into the cloud, it could be stored, organized and analyzed depending on where the processing power is needed to perform a function or achieve an analytic and actionable result. An analytic result from someone's smart phone, such as identifying the nearest Starbucks, requires that the smart phone serve as a sensor, propagator node and an integrator that leverages location information in the cloud. That information is immediately actionable. As soon as someone is holding that latte, they will forget about that transaction, but the IoT will not. That transaction is captured in the cloud and aggregated with other transactions which could be accessed by commercial entities or intelligence collectors who both may be interested in learning more about one's behavior to provide better purchasing services, or perhaps to identify and disrupt nefarious activities.

In the commercial on-line environment, speed matters. It also matters when law enforcement is attempting to disrupt a looming terrorist attack. The potential fleeting relevance of actionable data reinforces the perspective that data storage is necessarily a dynamic process that must occur to some degree at all three functional levels of the IoT, but particularly at the propagator nodes and in the cloud. Data use requirements include the speed in which data and analytics must translate into action, and dictate how much processing power and memory should be applied at each of those functional levels. For law enforcement entities to understand and react quickly to terrorist activity they need to possess superior processing power closer to the 'edge' of the IoT network. From a commercial perspective, however, it is less efficient to push power to the edge than it is to leverage the cloud. This suggests that the development of propagator nodes is critical as the law enforcement and intelligence communities consider how to potentially use commercial IoT data for intelligence purposes.

The challenges law enforcement and intelligence entities face in acquiring and using personal data to identify and track potential terrorists range from how, where and for what purpose IoT data is collected and processed and the different legal frameworks under which data is collected. These challenges are particularly acute when intelligence entities are trying to identify and track potential terrorists traveling from Hong Kong to San Francisco, especially during terrorist planning and reconnaissance activities that may occur remotely or within the target area. Varying accessibility rules, data handling procedures, storage capacities, and the diverse architectures and purposes of IoT networks will tend to make this analysis difficult even in the IoT. However, it will probably be less difficult in the foreign space than the domestic space depending on the level and pace of IoT adoption.

The Way Ahead

The IoT is here and it is transforming how we live and work. McKinsey Global Institute identified the IoT as among the most disruptive technologies of the decade. Cisco estimates that the IoT will consist of 50 billion devices connected to the Internet by 2020 with an additional million devices coming online every month. This new landscape is global and manifests itself in everything from smart cities to agriculture to governance. The IoT identifies us, feeds us, transports us, informs us, and keeps us safe. Given these transformations, leaders in government must know what is on the IoT horizon and start preparing for its impact on agency missions.

The IoT is being driven by the private sector and academia. It is imperative that the US government builds and sustains trust with these sectors and creates meaningful collaborative relationships through transparency and cooperation. All elements of government should foster and support standards to help build a secure, resilient IoT. The ODNI should also lead an effort to link IC component IoT experts and organizations together in a collaborative network to understand and leverage IoT. IoT technology will have significant implications for the intelligence enterprise and for the military and civilian components of government that the IC services. Understanding how IoT will impact the mission of those customers including the military and civilian agencies will be essential for the IC and warrant further study.

---

[1]McArdle, Elaine. "The New Age of Surveillance - Harvard Law Today." *Harvard Law Today*. Harvard Law Today, 10 May 2016. Web. 12 Aug. 2016.
[2]Dwoskin, Elizabeth. "What's Driving Silicon Valley to Become 'radicalized'." *Washington Post*. The Washington Post, 24 May 2016. Web. 12 Aug. 2016.
[3] Comstock, Jonah. "PwC: 1 in 5 Americans Owns a Wearable, 1 in 10 Wears Them Daily." MobiHealthNews. N.p., 21 Oct. 2014. Web. 16 Aug. 2016.
[4] NIST Information Technology Laboratory website, "NIST's Network-of-Things Model Builds Foundation to Help Define the Internet of Thing," July 28, 2016
[5]LotaData. *LotaData Announces Launch of Smart City Platform with San Francisco Bay Area Cities. Streetinsider.com*. N.p., 1 June 2016. Web. 12 Aug. 2016.
[6] Interview in San Francisco
[7] NewsStaff. "San Francisco Aims to Build Biggest Internet of Things in the U.S." *San Francisco Aims to Build Biggest Internet of Things in the U.S*. N.p., 23 Oct. 2015. Web. 12 Aug. 2016.
[8] Jenny Hogan, "Smart Software Linked to CCTV can Spot Dubious Behavior," New Scientist Magazine, July 11, 2003. www.newscientist.com/article/dn3918-smart-software-linked-to-cctv
[9] Lee, Kristen. "Healthcare IoT Security Issues: Risks and What to Do about Them." *SearchHealthIT*. N.p., n.d. Web. 12 Aug. 2016.
[10] "Barcelona Named 'Global Smart City – 2015'" - *Juniper Research*. N.p., 17 Feb. 2015. Web. 12 Aug. 2016.
[11] *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*, 113th Cong., 3 (2016) (testimony of James Clapper). Print.
[12] Pew Research Center, "Public Trust in Government: 1958-2015, November 23, 2015. WWW.people-press.org.
[13]"Twitter May Have Cut Spy Agencies Off From Its Flood of Data." *Wired.com*. Conde Nast Digital, May-June 2016. Web. 16 Aug. 2016.
[14] Payne, Larry. "Public Sector Is Embracing Silicon Valley and Everyone May Benefit." *Bloomberg Government*. N.p., 24 May 2016. Web. 16 Aug. 2016.
[15]Kryders law, (2005).http://www:chipwalter:com/articles/profiles/kryder

[16] Francis daCosta, "Rethinking the Internet of Things: A Scalable Approach to Connecting Everything," 2013, Apress Media, LLC, page 18.

All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.