Protecting Privacy in an **IoT-Connected World**

Michael S. Smith, Ph.D., IGP, CRM

To say we live in a connected world is an understatement in light of the growth of the *Internet of Things* (IoT), which is described in "Internet of Things Global Standards Initiative' by ITU – the United Nation's agency for information and communications technologies – as the network of physical objects embedded with electronics, software, sensors, and connectivity that enable them to collect and exchange data.

The Rise of IoT

Gartner says by the end of 2015, 4.9 billion connected things will be in use – up 30% from 2014. Three factors have played a significant role:

1. The development of the personal computer
2. Ubiquitous computing at low costs
3. Low-cost storage

A more recent business trend contributing to escalating data volumes is commonly referred to as SMAC, which involves using four major technologies – social, mobile, analytics, and the cloud – to engage with and collect data about customers, which is then analyzed and used to drive innovation, process improvements, and productivity.

IoT's Anticipated Growth

The number of IoT connections continues to grow exponentially: Gartner predicts 25 billion devices will be connected to the IoT by 2020. IDC predicts that in that same year, the "digital universe" will reach 44 zettabytes – that's 640.2 billion 64GB tablets full of data – by a world population that's projected to be fewer than 8 billion people, according to the July 2015 update to the International Data Base.

IoT's Daily Influence

The IoT is being leveraged by people and organizations across the industry spectrum for a variety of purposes, changing nearly everybody's daily lives, as shown in the following examples.

Personal Use

IoT connections can send an individual's blood pressure, glucose levels, and other medical metrics to doctors. Pedometers and health meters on smart watch devices also help people track and share their progress toward their personal health goals.

Sensors on cars alert emergency services to accidents, and responders locate accidents via geographic positioning systems.

"Smart" homes have thermostats that can be adjusted, lights that can be turned off and on, and garage doors that can be opened and closed via smartphone, refrigerators that can track food supplies through radio frequency identification tags and automatically order more, and washing machines that turn on when the demand for energy is low.

Introduced in March, Amazon's Wi-Fi-enabled Dash buttons can be located in kitchens, bathrooms, and garages, enabling users to reorder the products they use frequently in those locations with a single click.

Government Use

"Smart" cities are also a growing trend around the globe. Sensors combined with information and communication technologies run cities more efficiently and effectively, reducing costs and the consumption of valuable resources.

Singapore, for example, connects smart devices to taxi mirrors to monitor traffic congestion. The sensors feed data into a centralized hub and analytics predict traffic patterns and redirect traffic lights to improve traffic.

Global Use

The Organization for Economic Co-operation and Development's Digital Economy Outlook shows South Korea as the most-connected country, with 37.9 things connected to the Internet per 100 people. Interestingly, the United States is fourth at 24.9 per hundred. (See Figure 1 below.)

The Cost for IoT: Privacy

The real cost of the IoT may be greater than most people think. While most understand the potential threats of searching web pages and take steps to protect themselves with antivirus software, they may not understand the need for the same type of protection related to IoT use.

Smart Homes

That thermostat or security camera purchased to be controlled with a smartphone, for example, needs to be connected to the Internet to work, which opens the home to potential risks, including invasion of the residents' privacy.

"The appealing convenience of Smart Home devices comes with a sobering downside," writes Randy Southerland on *SourceSecurity.com*. "They can also send a steady flood of personal data to corporate servers, where it's stored and even shared with companies and individuals you don't know and over whom you have no control."

Southerland recounted the furor earlier this year that came from the revelation that televisions with features that control channels and volume by voice command also record conversations and could potentially send them to outside parties. The fine print in privacy policies, Southerland wrote, revealed this, as well as the fact that the function could be turned off.

Freemiums

A lot of personal information is proliferating from IoT devices and individuals subscribing to digital services, such as LinkedIn, Facebook, Gmail, and Snapchat, as well as

Rank	Country	Per 100 inhabitants
1	South Korea	37.9
2	Denmark	32.7
3	Switzerland	29.0
4	United States	24.9
5	Netherlands	24.7

Source: OECD Digital Economy Outlook 2015 available at h*ttp://dx.doi.org/10.1787/888933225312*

smartphone applications. These are known as *freemiums* – free services that many eventually pay a premium for to gain additional features and functionality.

People signing up for these accounts generally must agree to the providers' terms of use, which often comprise a long list of legalese that few read. Instead, users click "yes," oblivious to the privacy rights they may be forfeiting. Companies offering the free services are not intent on invading their users' privacy, but they are in the business of providing personalized data to organizations that will pay for it.

In this age of *quid pro quo*, or "something for something," these companies provide services in exchange for user information, which they scientifically aggregate, sort, and index in order to deliver personalized responses to their users. For example, the ads that pop up on users' screens are determined by complex algorithms and predictive analytics of data derived from the user's profile, preferences, browsing habits, and spending history.

According to the 2015 Altimeter Group study "Consumer Perceptions of Privacy in the Internet of Things," while the vast majority of consumers don't know what the term *Internet of Things* means, they know they have Internet-connected devices – and 45% of the respondents expressed very low trust that the companies are protecting the personal data they are collecting.

Consumers' Protection of Data

The IoT wave is moving much more rapidly than the right of privacy can be ensured. And although the U.S. Federal Trade Commission (FTC) has proposed federal law to address data privacy, and groups meeting at various summits, trade shows, and think tanks are coming together to address these concerns, consumers must own the responsibility for their data privacy.

Read More About It (accessed 19 Oct. 2015)

Gartner Inc. "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," November 11, 2014. *www.gartner.com/newsroom/id/2905717*

Higginbotham, Stacey. "Companies need to share how they use our data. Here are some ideas." July 16, 2015. *http://fortune.com/2015/07/06/consumer-data-privacy/*

ITU. Internet of Things Global Standards Initiative. July 1, 2015. *www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx*

Mejia, Paula. "Wary of Privacy Issues? Ditch Dropbox and Avoid Google, Says Edward Snowden." *Newsweek*, 11 Oct. 2014. *www.newsweek.com/wary-privacy-issues-ditch-dropbox-and-avoid-google-says-edward-snowden-276956*

National Strategy for Trusted Identifies in Cyberspace. "The Fair Information Practice Principles," February 2014. *www.nist.gov/nstic/NSTIC-FIPPs.pdf*

Organization for Economic Co-operation and Development. "OECD Digital Economy Outlook 2015," 29 May 2015. *http://dx.doi.org/10.1787/888933225312*

_____. "Guidelines on the Protection of Privacy," ammended 11 July 2013. *http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf*

Southerland, Randy. "Smart Home Security Risks with Internet of Things (IoT)." SourceSecurity.com U.S. edition. *http://us.sourcesecurity.com/news/articles/18159.html*

U.S. Federal Trade Commission. "Staff Report: Internet of Things: Privacy & Security in a Connected World," January 2015. *www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*

One man who infamously put privacy on the front page of newspapers around the world in 2013, U.S. National Security Agency whistleblower Edward Snowden, recently provided advice for how to protect your own privacy.

In an account of an interview with The New Yorker's Jane Mayer that was published online by Newsweek, Paula Mejia quoted Snowden as saying people should "search for encrypted communication services" because they "enforce your rights" and to be cautious about online services like Facebook, Google, and Dropbox, which he said are "hostile to privacy." He recommended using secure services to encrypt information and using online storage providers that care about privacy.

Consumers should document the accounts they have opened, review the providers' privacy policies, and review the information stored with or transmitted through these providers. If any of it is private, it might be time to reassess their use.

Further, document every "thing" connected to the Internet, as this could help track the source if any "leak" should occur.

Organizations' Protection of Data

Assessing personal privacy risks is a good first step in considering how to protect the privacy of the organization's internal and external customers and stakeholders. IG professionals need to ensure the organization has implemented and is in compliance with comprehensive security and privacy policies to protect private data.

In the FTC's January 2015 staff report "Internet of Things: Privacy & Security in a Connected World," the agency recommended data minimization as a way to balance data use with privacy protection. Organizations can decide not to collect data at all; collect only the data necessary to the product or service being offered; collect less data that is sensitive; or de-identify the data they collect. If none of these options works, the organization can seek consumers' consent for collecting "additional, unexpected" data.

IG professionals must ensure comprehensive internal compliance audits to confirm their organizations' adherence to the long-standing U.S. "Fair Information Practice Principles" (FIPP). Rooted in the seminal report on privacy issued in 1973 by The Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers and the Rights of Citizens," the FIPP are at the core of the U.S. Privacy Act of 1974.

OECD Guidelines

The FIPP also form the core of the widely accepted 2013 *OECD Guidelines on the Protection of Privacy*:

1. **Collection Limitation Principle**. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle**. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle**. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a. with the consent of the data subject; or
   b. by the authority of law.
5. **Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle**. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**. An individual should have the right:
   a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
   c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
   d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. **Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the principles stated above.

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

A Balancing Act

The vast volume of data being generated by the IoT is a double-edged sword of value and risk that must be balanced carefully. In this hyperconnected world, informed citizens must balance the benefit of using IoT with their need for protecting their privacy. Organizations that consume the vast supply of data the IoT generates must also balance the value of using that data against the risk of violating customer and stakeholders' rights to privacy.

It is the responsibility of IG professionals that their organizations do this by following the OECD Principles, recommending the collection of personally identifiable information be minimized, and ensuring compliance with applicable privacy laws. **END**

Michael S. Smith, Ph.D., IGP, CRM, can be contacted at mike.s.smith@charter.net. *See his bio on page 47.*