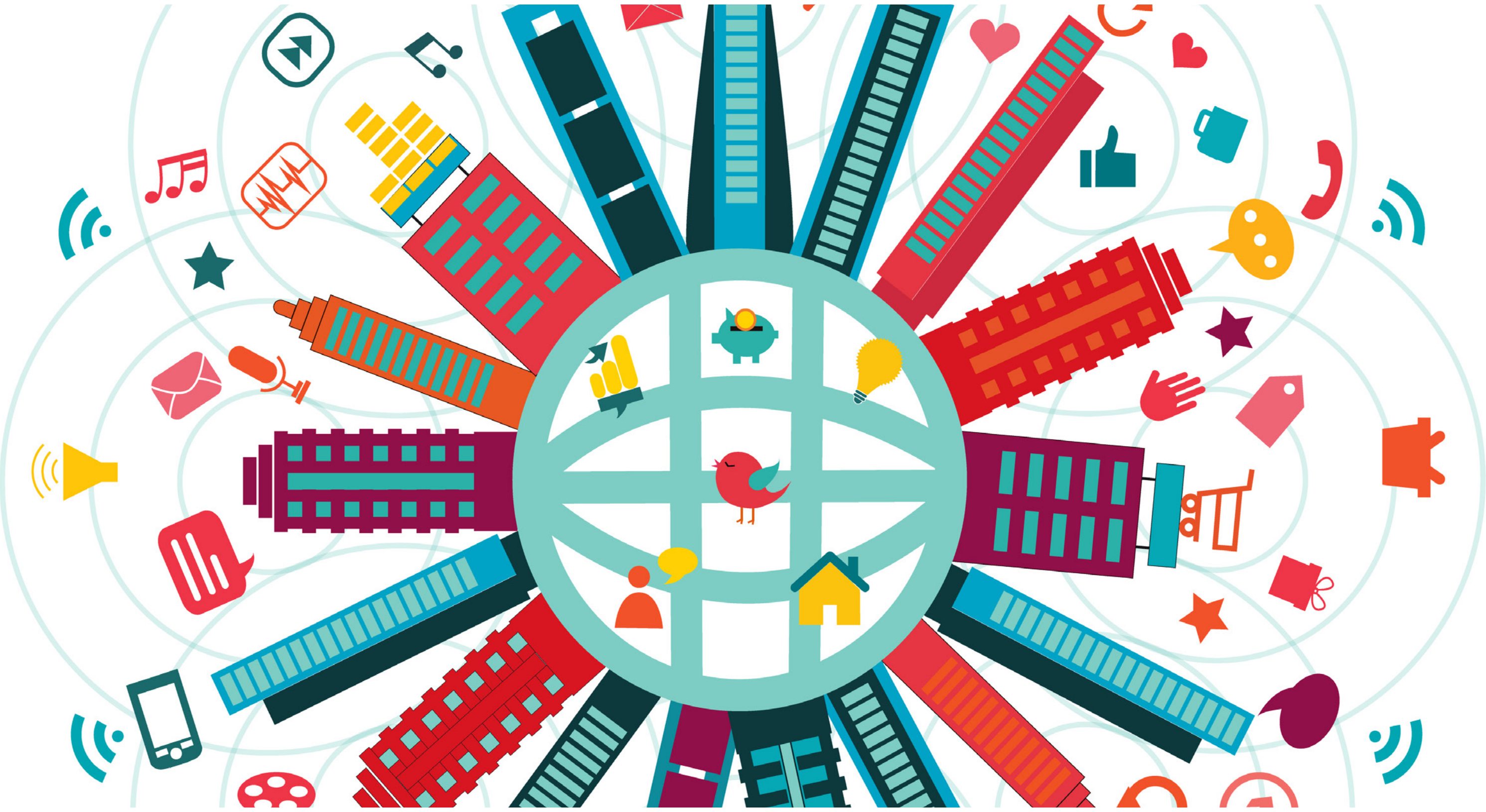
FOSI Briefs

Family Online Safety Institute

May 7, 2015

Everything Connected: Possibilities and Privacy

The advent of connected cars, interactive fridges and Internet-enabled watches brings with it a wealth of possibilities. However, the ways in which the new technology will simplify our daily lives, boost commercial profits and the innumerable life-changing opportunities that it presents must be balanced against the potential for invasion of privacy, data breaches and even misuse.



The Internet of Things has been defined by the Pew Research Center as "a global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive data centers in a world-spanning information fabric." To date there has been a proliferation of personal wearable health devices that count steps, monitor heartbeats and track sleep patterns. Internet-enabled systems installed in homes can control both the temperature and alarm systems, while the technology also allows for remote health monitoring and emergency notifications for the elderly. The impact of the Internet of Things is already evident in sensors on streets and in traffic lights, which have improved urban management. In the near future, more and more devices will be able to connect to the Internet, resulting in improvements in corporate logistics, enhanced manufacturing processes and personal productivity.

At a recent event held by FOSI on the Internet of Things the actual and potential effects of this technology to improve the lives of disabled users were highlighted. The advancements in medical treatments offered by mass data collection and use of cameras in surgical procedures have improved the prognosis of many illnesses. The independence that can be afforded to a disabled or elderly person living alone through the use of environmental controls, sensors and remote monitoring can change their lives drastically. In return for these immeasurable benefits, many disabled people are willing to give up more of their data and potentially compromise some of their privacy, but does it have to be a choice? Privacy or technological advancement?

Privacy advocates, regulators and lawmakers around the world have begun to grapple with some of the challenges presented by this new technology. Specific concerns have been expressed about the amount of data being collected and often it's intensely personal nature. Medical and biometric information has long been afforded special protections, but what happens when it is being uploaded from a device that is worn 24/7 by an individual using it to improve their health? The risk of data-breaches, misuse by commercial entities and exploitation by bad actors are just some of the causes of unease about the Internet of Things.

An absence of user control or awareness of the data collected, excessive amounts of unnecessary information being stored, the removal of freedom of choice by requirements to consent and a lack of anonymity have also been raised as potential issues. Who is best placed to respond to these challenges has been heavily debated. Is it government, industry, civil society or the individual? The need to avoid legislation limiting innovation has been acknowledged, but further concerns are real and may require a response.

In the United States, Capitol Hill and the Federal Trade Commission (FTC) have reacted to the emergence of the new technology, and to the apprehension that it has caused. In Congress, numerous hearings have taken place, with policymakers weighing the benefits of the technology against the potential risks. Thus far the indications have been that there is support for a system of best practices and reliance upon current regulation, rather than proposing new laws.
The Federal Trade Commission, the consumer protection agency in the US, released its report entitled "Internet of Things: Privacy & Security in a Connected World" in January 2015. The findings came about as a result of a workshop on the Internet of Things in 2013 and in addition to the summary of the workshop discussion the FTC staff make numerous recommendations. At the same time the FTC released Careful Connections providing guidance to companies encouraging them think through implications of connected devices, including privacy by design and adequate and informed staff.

The FTC report advised companies developing this technology that they should implement reasonable security practices, consider data minimization as standard, and prioritize notice and choice for consumers. However, ultimately the Commission concluded that specific legislation for the Internet of Things was unnecessary, but staff reiterated their past calls for technology-neutral legislation allowing the FTC to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. Currently Section 5 of the Federal Trade Commission Act covering "unfair or deceptive acts or practices in or affecting commerce" allows the FTC to regulate the Internet of Things in the United States.

Furthermore, although the Internet of Things has yet to fully expand to impact children's lives, it not far off. Already there are dolls that connect to the Internet and allow children to fully interact with their toys. The doll even 'remembers' things that the child has said and will refer back to it overtime. Concerns have been raised about the safety and privacy implications of these devices recording and interacting with children. Data collection from those under the age of 13, without parental consent, violates the Children's Online Privacy Protection Act (COPPA) in the US, and this legislation equally applies to the Internet of Things.

In Europe, the European Commission is paying close attention to developments, while in the United Kingdom, the Government's Chief Scientific Adviser published a report in December 2014 making various recommendations. "The Internet of Things: making the most of the Second Digital Revolution" cautioned against 'trivialising' the impact that the technology could have on society, and downplayed the need for specific legislation. In addition to highlighting the importance of 'security by default' and data protection, it called for the UK government to promote a clear vision for the Internet of Things, and to establish an advisory board to foster collaboration between government and industry.

The potential impact of misguided legislation on this developing industry is widely recognized. That is not to say that there should not be standards and guidelines. Best practices and basic requirements should be developed through cooperation of many stakeholders, but it should by lead by industry.

As with any new technology, the importance of building and sustaining consumer trust is vital. Fears around the possibility of data breaches and the misuse of information have been raised by a number of different bodies. These concerns are genuine, and most companies should take their data protection responsibilities seriously. If they lose consumer faith at this early stage, it will be extremely difficult to regain it. The impact that this would have on the developing Internet of Things industry would be much more catastrophic than almost any of the legislation that could be proposed.

As the Internet of Things industry develops, it is important that privacy standards are built in from the beginning. Given the sensitive nature of the information that is collected, not to mention the access that the sensors have to almost every aspect of a person's private life, means that privacy by design is essential and cannot be an afterthought. The lessons that have been learned to date show us that you cannot have true privacy without security and that too must be incorporated at an early stage of development.

The importance and viability of fully informed consent, data minimization and de-identification of data should be explored. Consumer control and transparency are also vital to maintaining consumer trust, imperative for this new omniscient technology.

Legislation, industry best practices and agency guidelines can only go so far. The best and only real way to ensure safety and privacy in a new connected world is through education. Teaching children, and consumers of all ages the importance of protecting their information and making informed choices about the services they use will better protect them, while maintaining the limitless possibilities of new technology. The Internet of Things does not have to be a zero-sum game. The benefits can and should be afforded to all while minimizing the risks.

Emma Morris
International Policy Manager
emorris@fosi.org

About FOSI

The Family Online Safety Institute is an international, non-profit organization which works to make the online world safer for kids and their families. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.