Embedding Privacy Into What's Next:

Privacy by Design for the Internet of Things

Ann Cavoukian, Ph. D.
Executive Director, Privacy and Big Data Institute, Ryerson University

Claudiu Popa,
Executive Director, KnowledgeFlow Cybersafety Foundation

April 2016

KNOWLEDGEFLOW
CYBERSAFETY FOUNDATION

Ryerson University

Privacy &
Big Data
Institute

mobile | web | devices | wearable | cloud | social | smart | collaboration | appliances | search | advertising | sharing

Table of Contents

THE INTERNET OF THINGS NEEDS PRIVACY AND SECURITY

Ann Cavoukian

Imagine a world where everything is connected – not only online, but also in the physical world of wireless and wearable devices such as Fitbits, Nymi bands, Google Glass and Apple Watch – with a linking to connected cars, planes, trains and places.

If one adds to that the tracking of activities from one's monitored home by way of automated thermostats, light fixtures, smart TVs, smart meters and the smart grid, it will lead to the portrayal of the "quantified self," complete with the personal details of lifestyle, habits and activities all tracked and recorded. And one's entire lifestyle, containing a detailed set of activities and preferences, would potentially be accessible for all to see and, through the power of "machine learning," to analyze and make predictions about one's future behaviour.

Welcome to the Internet of Things, or perhaps more aptly, the Internet of Everything. Is this what we really want? Will the future world we live in be devoid of any privacy, upon which our individual freedoms are built? Because that is precisely what we have to consider – all that connectedness will pave the way for the surveillance of our lives, at an unimaginable scale. A scale that was aptly described by the director of U.S. national intelligence, Mr. James Clapper, when he indicated that intelligence services would soon use the IoT for identification, surveillance, monitoring, tracking, targeting and accessing networks.

But it doesn't have to be that way. If we embed privacy into the design of these inter-connected devices and programs, we can have the best of both worlds: privacy and the IoT.

Surveillance is the antithesis of privacy, and accordingly, the antithesis of freedom. But the good news is that neither privacy nor the benefits inherent in the emerging IoT have to be sacrificed. We need only abandon the limiting either/or, zero-sum thinking that posits you can only have one interest or another.

It will be difficult. This flawed line of thinking is so deeply engrained in our thought processes that trying to give it up poses a serious challenge. But by replacing the limiting "versus" with the power of "and," both interests – privacy and the IoT – may co-exist simultaneously in a win/win scenario, as opposed to the win/lose model to which we have become so accustomed.

This can be accomplished by embedding or coding privacy preferences into the technology itself, in order to prevent the privacy harms from arising. This is eminently within our reach, as the engineering and tech communities have repeatedly told me. No doubt, it will require innovation and ingenuity, but if we are to continue with existing technological progress in an increasingly connected world, it will be essential to maintain our future privacy and freedoms. It will also require foresight and leadership, in an effort to reject unnecessary tradeoffs and false dichotomies.

Privacy by Design is a framework I created for preventing privacy harms by embedding the necessary privacy protective measures into the design of information technology, networked infrastructure and business practices. It was unanimously passed as an international framework for privacy and data protection in 2010. Since then, it has been translated into 37 languages, giving it a true global presence. But nowhere is it needed more than in the emerging world of the IoT.

If we are to preserve any semblance of privacy in such a world, we must ensure that it is built into the very systems that are being developed. Otherwise, the interconnected nature of virtually all that we do may lead us down a path of surveillance that will be too great to conquer after the fact.

But it doesn’t have to play out that way. We can have privacy and the Internet of Things. But only if we speak up and reject the zero-sum status quo. As the Internet of Things heats up, we must support the growing number of great organizations that work to protect our right to privacy including the Canadian Privacy Commissioners at all levels of government, the U.S. Federal Trade Commission, UK’s Information Commissioner’s Office, European Parliament, Online Trust Alliance, Deloitte and the KnowledgeFlow Cybersafety Foundation.

I invite you to discover the Privacy by Design for the Internet of Things framework and encourage you to infuse your technology with the Principles and concepts presented here. I hope you choose to explore the incredible potential of responsible design and reap the benefits privacy-centric technologies.

This article, by Dr. Ann Cavoukian, executive director of the Privacy and Big Data Institute at Ryerson University, and former information and privacy commissioner of Ontario, originally appeared in the Globe and Mail.

http://www.ryerson.ca/pbdi/

DO THE PbD PRINCIPLES APPLY IN THE IOT AGE? YOU BET![1]

The 7 Foundational Principles of *Privacy by Design*

1. Proactive not reactive; Preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

[1] As illustrated in 2014 by the many good findings, safeguards and resolutions established as part of the “Mauritius Declaration on the Internet of Things” at the 36th International Conference of Data Protection and Privacy Commissioners: Privacy by Design is essential in the Internet of things.

A TIMELY PLAYBOOK FOR INNOVATION

Claudiu Popa

When I set out to help organizations adopt privacy I anticipated that the concept is too fluid and immaterial to be consistently applicable across organizations, industries and markets. I found Privacy by Design to be a fantastic resource for the boardroom, but its Principles didn't translate as well in a bottom-up fashion as they did top-down. That's okay, but privacy needs champions, and champions need a playbook.

That playbook turned out to be Privacy by ReDesign (PbRD), a set of standardized project management practices aligned with Privacy by Design but applicable by professionals at any level. Most importantly, the framework does not need to be brought in at the concept stage nor does it require a teardown of existing infrastructure. That wouldn't work and it would force organizations to counterproductively adopt a smoke and mirrors approach to privacy. Instead, it layers privacy practices and eases security controls into the fragile environments our enterprises depend on every day. The framework puts the project into the hands of professionals, slices it into pieces and strives for incremental improvement. It works.

While redesigning privacy works well for layering in security and privacy, it is necessarily operational and eschews a focus on the soft side of protection. Cybersafety by Design was built to lead with professional integrity, design ethics, user experience and opportunities to prevent abuse, and I ensured that it remained solidly anchored in Privacy by Design Principles. This allows it to be used to prevent cyberfraud, defuse online bullying, enable trolling detection and augment usability. It's a great way to build good technology well.

And building technology well is perhaps the most important aspect of responsible IoT design. The new paradigm will require nothing short of advanced tools, new approaches and combinatorial skill sets. The 50 billion devices estimated to be connected over the next 5 years will need a certain amount of awareness, perhaps even intelligence, but also respect for humans.

The 7 PbD Principles inspired IoT specific concepts that outline ways for technologists, innovators, finance professionals and individual consumers to fine-tune their expectations of this new era of design. The new focus will be on making technology useful, transparent and trustworthy for those whose existence it is intended to ameliorate. The rest is up to regulators, the public and people like you and me, 88% already demand to understand and control the data being collected through smart, connected devices.

Claudiu Popa is a privacy and security technologist, and the author of Managing Personal Information, CEO of Informatica Corporation and Executive Director of Canada's KnowledgeFlow Cybersafety Foundation. He used Privacy by Design to build Privacy by ReDesign and Cybersafety by Design, two platforms that vastly expand the reach and applicability of Privacy by Design into the real world.

http://www.knowledgeflow.ca

THE 7 FOUNDATIONAL PRINCIPLES: AN INTEGRATED FRAMEWORK FOR PRIVACY AND THE INTERNET OF THINGS

Principle #1: Proactive not reactive; Preventative not remedial

IoT Privacy Concept: Anticipate and Eliminate Opportunities for Abuse

The web of devices already connected and interconnected today is only a fractional part of the universe of technologies that will form the Internet of Things in the coming years. These devices will soon outnumber people, strain[2] the land-based Internet's capacity and take to the skies to transfer information in real time. For all its future benefits, the Internet of Things must use today as a baseline. This world where purpose-built devices don't need information sharing to work must be the baseline for information sharing into the future.

We must use proactive measures to anticipate privacy challenges. That means the value we get today from a toaster with zero intelligence and capacity for data collection must always be weighed against future appliances that offer added convenience with the caveat of increased information sharing. Anticipating such advances may be easy, but innovations must always refrain from assuming what the public wants from technology and force themselves to simply ask. Consent will be the greatest challenge to privacy abuses in the future Internet of Things.

Principle #2: Privacy as the default setting

IoT Privacy Concept: Configure Privacy by Default

Building safeguards into innovative technology solutions, educational programs and social networking must not be seen as a distinctly different development life cycle process. Intrinsically designing privacy into all innovations before information management capabilities are added is the best way to foster trust and encourage full use of the resources made available by tomorrow's connected products. When consumers are able to rely on the knowledge that their safety is protected, that degree of assurance is the very mechanism that will unlock the promise of tomorrow's technology ecosystems.

In-built integrity must rub off from the designer into the product to breed the confidence to strengthen brands and create the good will necessary for adoption. Enthusiastic consumers will always support the technologies that support their ideals. Default privacy and integrity in the Internet of Things don't just add layers of data protection, they make progressive organizations look good ... and for good reason. Those organizations will benefit from a very real public perception gap that will always favour trustworthy technologies over rapacious data collection practices.

[2] Estimates for the number of connected devices in 2020 range from 21 billion (Gartner) to 34 billion (Business Insider) to 50 billion (Statista).

Principle #3: Privacy embedded into design

IoT Privacy Concept: Embed Integrity into Design

Consistently embedded privacy into IoT technologies means seriously treating the responsibility to protect user information at *all* levels. A real commitment to privacy means integrity, not manufactured demand and market influence, drive product design and engineering. The Internet of Things will include increasingly intelligent devices competing for bandwidth, data and attention. If the repeatable, reliable and consistent application of information management brings about increased sentience, responsible design will necessarily include privacy and integrity to form the strong fabric of tomorrow's society, in which intelligent devices will seamlessly interface with, augment and enhance human existence.

Instead, layering and inserting privacy into layers of IoT is of paramount importance to preventing abuses and anchoring protection early on. Those early layers represent bottom-up functionality that make sense to good designers, will thrill developers and create a sense of security among customers.

Principle #4: Full functionality – positive-sum, not zero-sum

IoT Privacy Concept: Fuse Optimized Experiences to Full Functionality

Fostering consumer interactions and experiences that infuse trust into relationships begins with the end goal. A world where users must choose between privacy and security, or accept surveillance in exchange for safety is not a positive sum solution to the social problems of the day. To create a win-win scenario, thinking bigger, introducing innovations that maximize user experiences while protecting user interests represents a solid, principled approach.

Functionally effective safeguards are unobtrusively designed to provide the comfort to take in value offered by legitimate programs, systems and networks. Embracing public interest means delivering solutions that are not *limited* by the natural need for safety and security, nor curtailed by the human right to privacy. Reducing the richness of feature sets reduces user experiences and ultimately limits the potential to effectively reach greater communities and satisfy more audiences.

Principle #5: End-to-end security – full lifecycle protection

IoT Privacy Concept: Clarify & Simplify for Protective Design

Complexity is the enemy of usability. The online world's dependence on a reactive model where transparency reports, terms of service, privacy and security policies have become the norm, the clear goal needs to remain the provisioning of effective solutions that mitigate the risk of abuse.

Privacy by Design for Internet of Things begins with a simple message clearly articulated and easily accessible throughout the entire design and user experience. User awareness and security assurance are the building blocks of the most comprehensive solutions but it is that full lifecycle protection that ensures privacy. The scalability of approaches for safe use of technology in family settings, for complete user-centricity in systems development and for responsible engineering in discrete environments are the keys to effective consumer protection. Organizations, industrials and developers that adopt privacy best practices can therefore ensure the consistent, end-to-end application of simple but overlapping security measures that effectively represent the foundation of tomorrow's trusted Internet of Things. The alternative is not an option.

Principle #6: Visibility and transparency – keep it open

IoT Privacy Concept: Control Monitoring and Awareness

The Internet of Things was borne of open design. By design, privacy principles embrace an overlapping but transparent mesh of privacy protective measures intended to eliminate opportunities for abuse. As a layered approach, Privacy by Design's inclusive model ensures awareness, encourages responsible use and enhances the relationship between innovator and consumer.

To do so, technologists must know where the line is between protective monitoring and opportunistic surveillance. Treating audiences as stakeholders whose needs for security and safety must be respected above all else is a fundamental approach. Effective controls must be tempered with responsible monitoring. Collected information must be shared with the people it was collected from. Practices must be compatible with independent verification to generate trust. Without these concepts, even the most innovative initiative will squander the traction, value and trust it was originally created to garner. Flexibility, visibility and transparency are some of the key notions used to combat Fear, Uncertainty and Doubt (FUD), and it is critical that they be in-built at this early stage in the process.

Principle #7: Respect for user privacy – keep it user-centric

IoT Concept: Include Users as Stakeholders, not Victims

Data collection is about respecting users and consumers. In the evolving Internet of Things, every individual is a content generating node. Such notions can lead innovators and engineers on a path away from privacy protection. Responsible Internet of Things solutions must necessarily address a problem, but beyond that, they must demonstrate respect for the public in their collection and handling of information. Surreptitious acquisition of intelligence has no place in responsible design.

If we are to leverage public trust as a quantifiable asset then users must be stakeholders, not victims. For that, engineers must leverage Privacy Principles as a springboard to good implementation that shares, not obscures its activity. This approach is the glue used to build the bonds of confidence and create trust-based ecosystems. By architecting non-invasive technology platforms that encourage the responsible use of information, builders can scale individual user relationships into vast networks for information exchange, knowledge transfer and personal growth ... on a vast scale. The notions of users as stakeholders – not unwitting victims - are intrinsic to privacy protection. These once abstract ideas are today very real, with damaging consequences that can only be alleviated by the systematic, assiduous application of controls that protect not only the most vulnerable, but every single, valuable member of each user base, every citizen of our online society and every element in our growing ecosystem of interconnected people & devices - the Internet of things.

DESIGN METHODOLOGY

The design of products and solutions within the greater Internet of Things space must necessarily be innovative, useful and effective, but to subscribe to principles of good design it must also be thorough and detailed, unobtrusive and aesthetic, socially responsible and *honest*.

This approach meshes well with Privacy by Design, where user-centricity, openness and design integrity are valuable principles that need to be fundamentally adopted to ensure protection and trust.

In broad strokes, systematic design for IoT depends on the application of Privacy by Design using tools, techniques and processes that may not yet be in existence. Yet the principles upon which all such products and solutions will base their operational integrity has existed for decades and it is only a matter of ensuring their fit from an engineering perspective.

The authors encourage organizations, associations, groups and individuals in all sectors to use the PbD Principles for IoT Design framework in building, unveiling and scaling disruptively ambitious and overwhelmingly beneficial opportunities that contribute to the rising tide of responsible engineering and consumer-centric design.

ENGINEERING PRIVACY FOR GOOD DESIGN

While the Internet of Things moves from hype to maturity, industrial innovators have already begun to make inroads into standardized techniques and operating guidelines for the introduction of simple, useful and attractive products for future decades.

Now is the time to adopt the privacy principles that will effectively and elegantly spearhead consumer-centric design for the next few decades. Use the sample questions below to align your objectives with those of your audience. Create a privacy document that will practically map these principles to concrete approaches. Demonstrate to test audiences how responsible design leads to robust engineering and enhanced experiences. Finally, implement a knowledge sharing program with your product and software designers, project and program managers, marketers and promoters. It will create a cohesive web of consistently dependable information protection that renders and improves your core security controls.

The IoT Privacy Principles form a framework designed to scale to support your scope. You need to rally the right core group of people, awaken their talent and focus on what the audience deserves for themselves and those around them. Proactive design, default protection, inbuilt privacy, open, transparent, secure implementation. It's the best way to have a far reaching impact using a simple approach that is widely adopted. The rest is up to you.

Operational Application of PbD Principles to IoT

1. **Anticipate** and Eliminate Opportunities for Abuse
2. **Configure** Privacy by Default
3. **Embed** Integrity into Design
4. **Fuse** Optimized Experiences to Full Functionality
5. **Clarify** & Simplify for Protective Design
6. **Control** Monitoring and Awareness
7. **Include** Users as Stakeholders, not Victims

CONCLUDING THOUGHTS ON TRUST, ANONYMITY AND THE INTERNET OF THINGS

With the Internet of Things and an imminent hyperconnected world soon composed of an estimated 26 billion devices[3] and intelligent appliances, what will become of our notion of trust? Will we ask fewer questions before surrendering personal information or submitting to automatic monitoring, or will we insist on adherence to basic norms of conduct for future technologies? Will our children consider their personal information a valuable asset to be used as currency in exchange for valuable services? Will our social ecosystems provide opportunities for connecting and monitoring everyone, all the time, or will they routinely incorporate the IoT privacy concepts based on the principles of Privacy by Design?

Time will tell. Instead of waiting however, we must heed the warnings and revisit the resolutions of the Data Protection Authorities that, in 2014 came together in Mauritius to warn about the sensitivity, value, transparency, processing, security and control of collected data[4].

We invite you to find ways to adapt and implement PbD privacy principles to current and emerging issues in your life. From surveillance to privacy abuses, all user risks arising from the use of mobile apps, devices or connected toys arise from the basic failure to implement controls and safeguards to ensure data protection.

You see opportunities every day. Create innovative tools, apply the Principles, help close the gaps. Why not help to expand and operationalize the Privacy by Design for the Internet of Things Framework into a more complete body of work? Embed privacy in your design and strengthen the fabric of our digital ecosystems. You can make a difference *today* on the Internet of tomorrow. Participation in the IoT is not a game played by different rules[5], but an opportunity to bolster data protection for future generations.

KnowledgeFlow Cybersafety Foundation

[3] TRUSTe Privacy Index

[4] IAPP coverage of the 2014 Mauritius Resolutions

[5] The Article 29 Working Party on IoT and the new proposed EU Data Protection Regulation