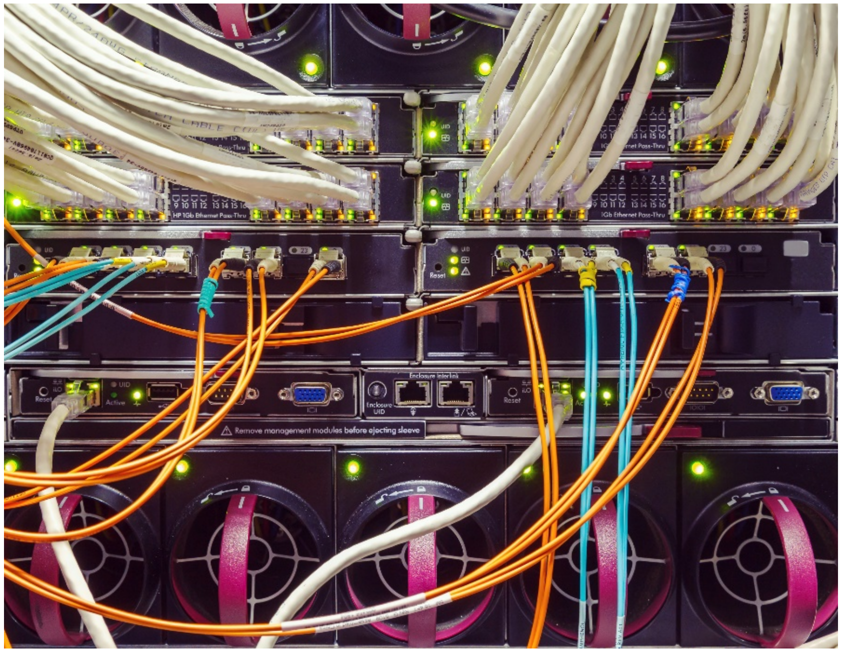
Deloitte.

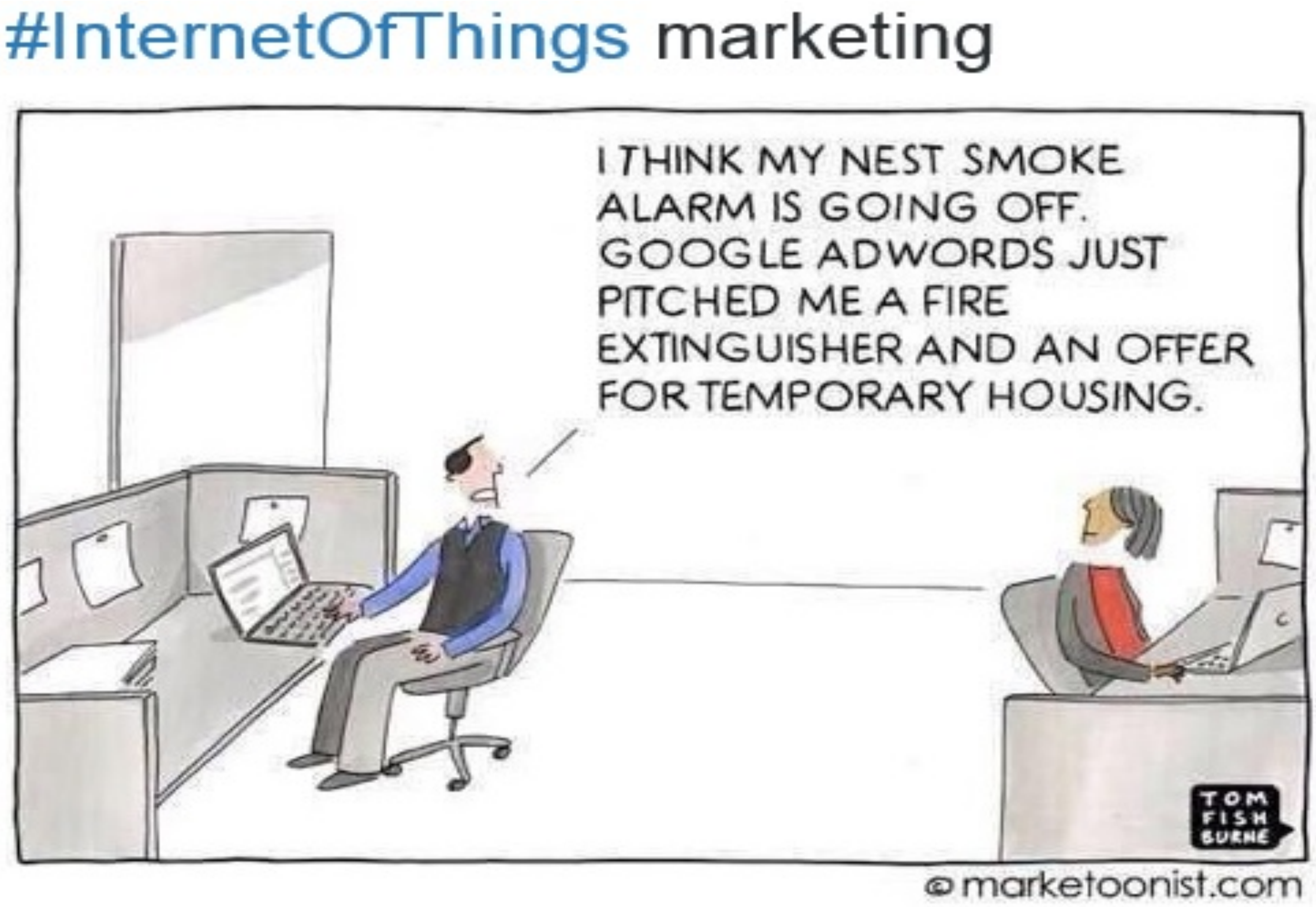
Managing Privacy Risk in the Age of the Internet



Sylvia Kingsmill, National Partner
Data Protection and Digital Privacy Leader

November 12, 2015

Let’s talk about privacy….


#InternetOfThings marketing
I THINK MY NEST SMOKE ALARM IS GOING OFF. GOOGLE ADWORDS JUST PITCHED ME A FIRE EXTINGUISHER AND AN OFFER FOR TEMPORARY HOUSING.
TOM FISHBURNE
© marketoonist.com

What is the Internet of Things (IoT)?

Automotive / Transportation

- Dealership of the future
- Remote diagnostics
- Fleet management
- Smart car

Manufacturing / Supply Chain

- Wireless factory
- Preventative maintenance
- Supply chain

Energy & Resources

- Smart grid
- Wellhead optimization
- Autonomous Mining

Military

- Connected battlefield
- Supply chain

Consumer

- Wearables
- Smart thermostat
- Smart home
- Smart alarm system

Financial Services

- Perf-based Insurance
- Personalized risk profiles
- Online banking
- Digital wallet

Retail / Vending

- Tailored offers
- Inventory management
- Checkout optimization
- Supply chain

Healthcare/ Lifesciences

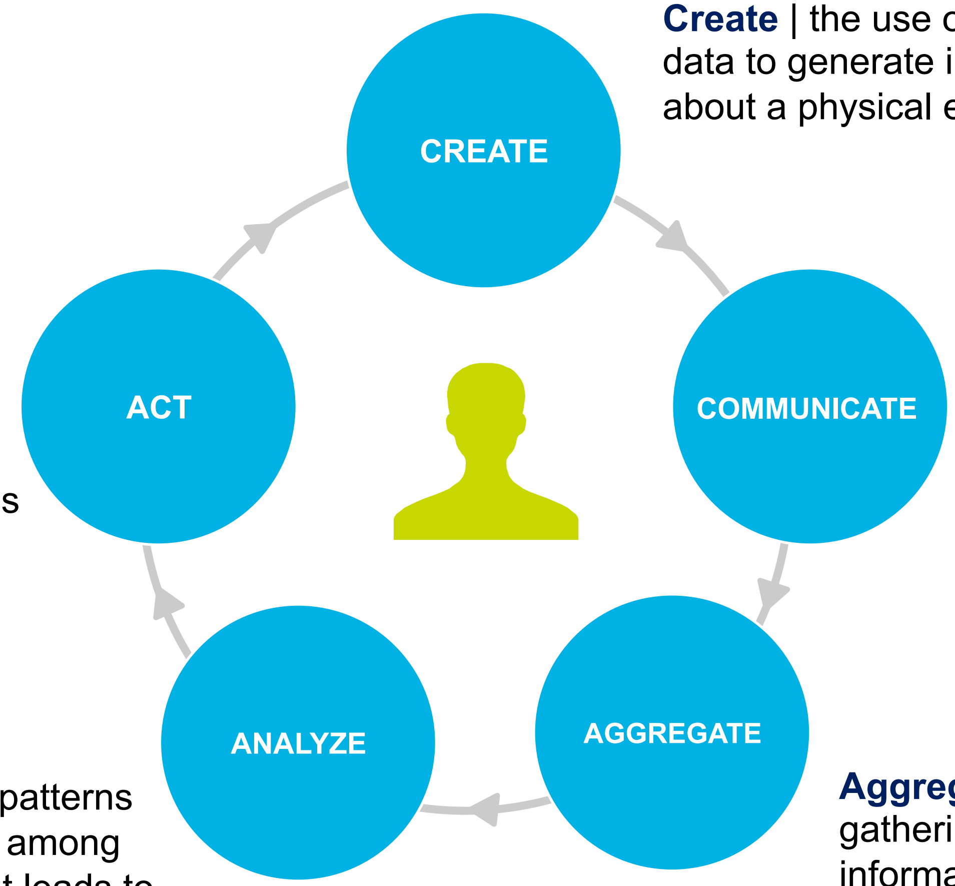
- Remote monitoring
- Patient experience
- Equipment monitoring
- Patient care
- Medical devices
- Bio wearables

Smart Cities

- Smart lighting
- Smart parking
- Smart waste
- Smart meter

***"Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion"** – Dave Evans, CISCO*

The information value loop – creating value from information



Create | the use of sensors and data to generate information about a physical event or state

Communicate | the transmission or information from one place to another via networks

Aggregate | the gathering together of information created at different times or from different sources

Analyze | the discernment of patterns or relationships among phenomena that leads to descriptions, predictions, or prescriptions for action

Act | initiating, maintaining, or changing a physical event or state – machines can make decisions based on aggregate data that is analyzed

Smart Cars

- Fully self-driving cars are expected to be on the market within 10 years
- Capable of sensing their environment and navigating without human input using technologies such as radar, GPS, and computer vision

Benefits

- Sensors on a car can notify drivers of dangerous road conditions
- Safety and convenience by taking human error out of the equation
- Wireless software updates, no need for dealership service
- Real time vehicle diagnostics to drivers and service facilities
- Automatic alerts to first responders when airbags are deployed or accidents occur
- Fully connected with smart phones for convenience

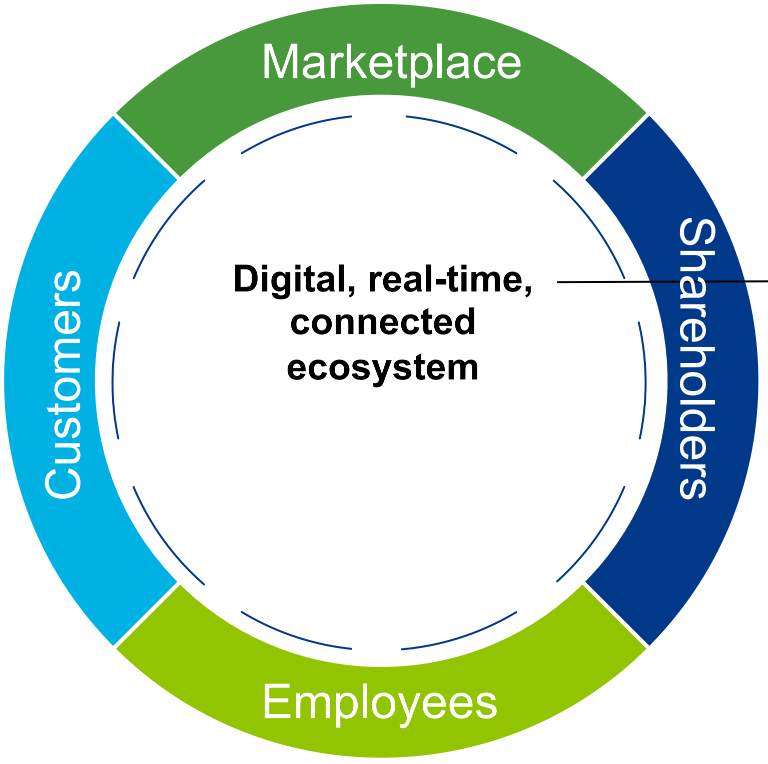
Wearables

- Wearable technology includes to a wide variety of devices from smart watches and glasses to smart clothes.
- Wearable technology enables a wide range of activities, which in turn enables a highly integrated customer experience

Benefits

- Enables new services that suit changing customer lifestyles
- Enables assessment of customer preferences which contributes to new and better software and technology
- Reduce costs from health insurance companies for good health behaviour
- Vital signs can be monitored without having to be at a doctor's office
- Connected health care devices can provide treatment options that can be independently managed
- Ease of sharing information to doctors or nurses, which can improve disease prevention, better drug management, and drive costs down due to a more efficient health care system

The Digital Enterprise



Marketplace

Customers

Shareholders

Employees

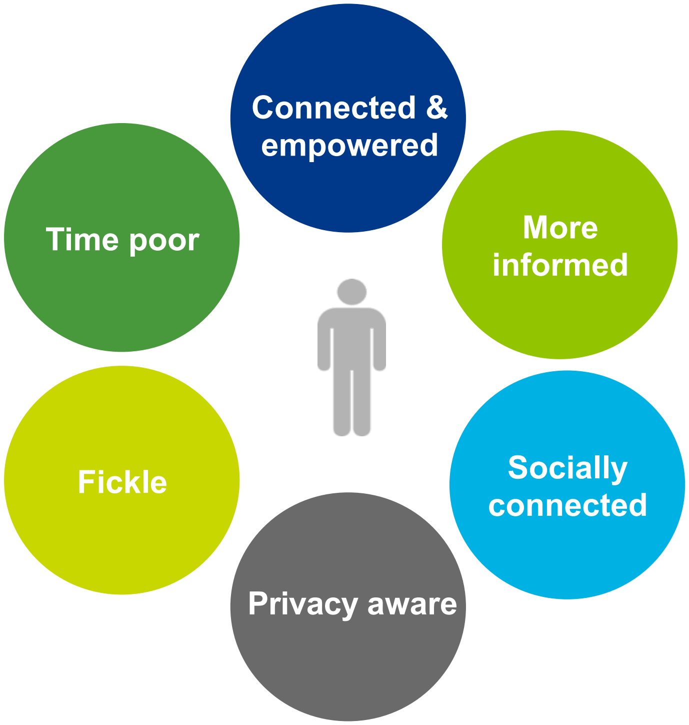
Digital, real-time, connected ecosystem

Disruptors

- Data science/machine learning for self defining models, artificial intelligence (AI)
- **Big Data** for processing unstructured (and structured) data
- **Internet of Things** deploying new sensors and signals to mine for new insights

The Digital Enterprise – our evolving version of where business is heading in the next few years. Already, mobile advances have put incredible technology in everyone’s hands. Social networks enable people to connect in ways never before possible. The cloud is drastically reducing the costs associated with hardware and data infrastructure, while data storage capabilities grow ever larger and ever cheaper. Data analytics can now make sense of vast amounts of data to provide valuable, actionable insights.

The connected consumer



Connected & empowered

More informed

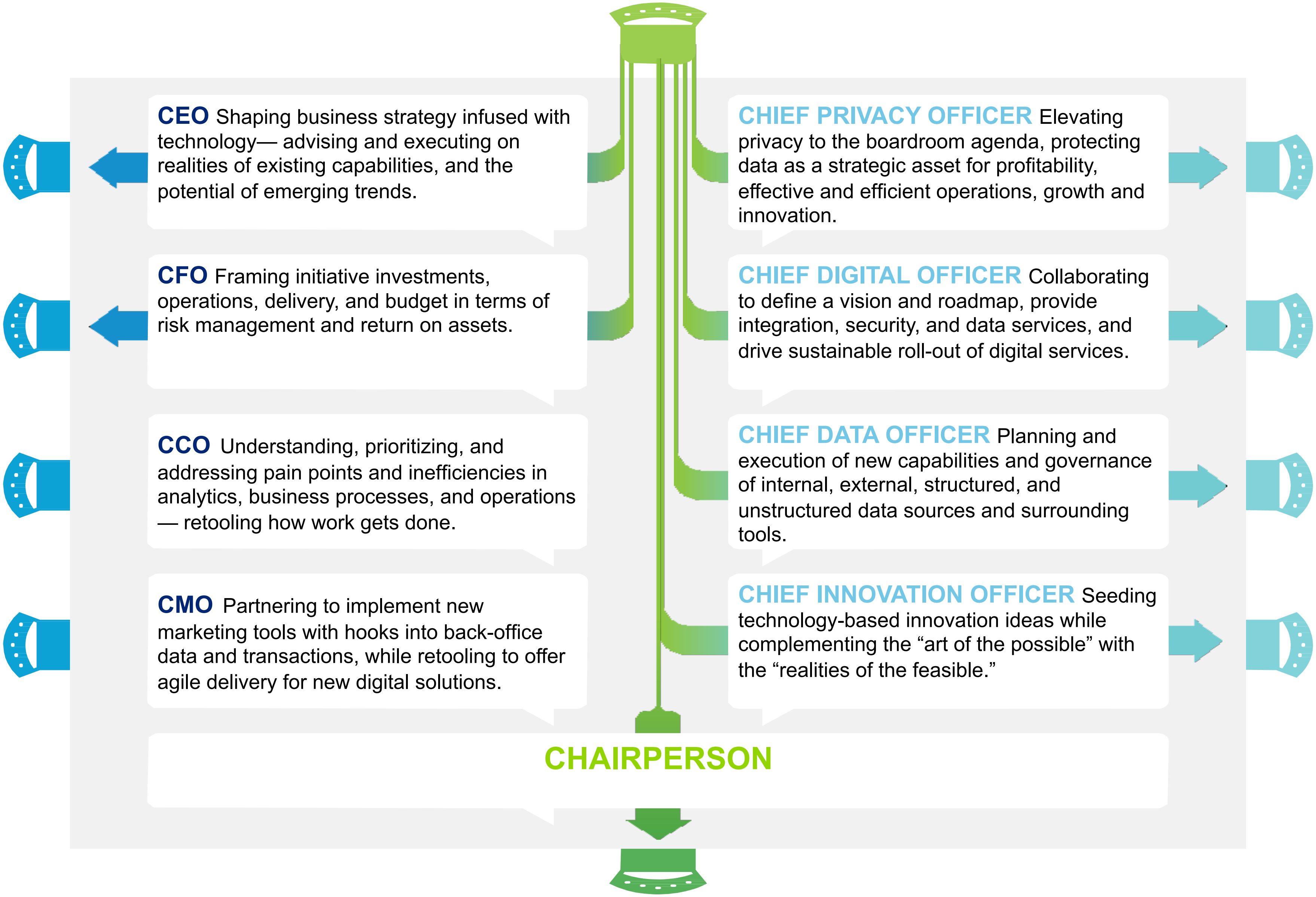
Socially connected

Privacy aware

Fickle

Time poor

New boardroom discussion



CEO Shaping business strategy infused with technology— advising and executing on realities of existing capabilities, and the potential of emerging trends.

CFO Framing initiative investments, operations, delivery, and budget in terms of risk management and return on assets.

CCO Understanding, prioritizing, and addressing pain points and inefficiencies in analytics, business processes, and operations — retooling how work gets done.

CMO Partnering to implement new marketing tools with hooks into back-office data and transactions, while retooling to offer agile delivery for new digital solutions.

CHIEF PRIVACY OFFICER Elevating privacy to the boardroom agenda, protecting data as a strategic asset for profitability, effective and efficient operations, growth and innovation.

CHIEF DIGITAL OFFICER Collaborating to define a vision and roadmap, provide integration, security, and data services, and drive sustainable roll-out of digital services.

CHIEF DATA OFFICER Planning and execution of new capabilities and governance of internal, external, structured, and unstructured data sources and surrounding tools.

CHIEF INNOVATION OFFICER Seeding technology-based innovation ideas while complementing the “art of the possible” with the “realities of the feasible.”

CHAIRPERSON

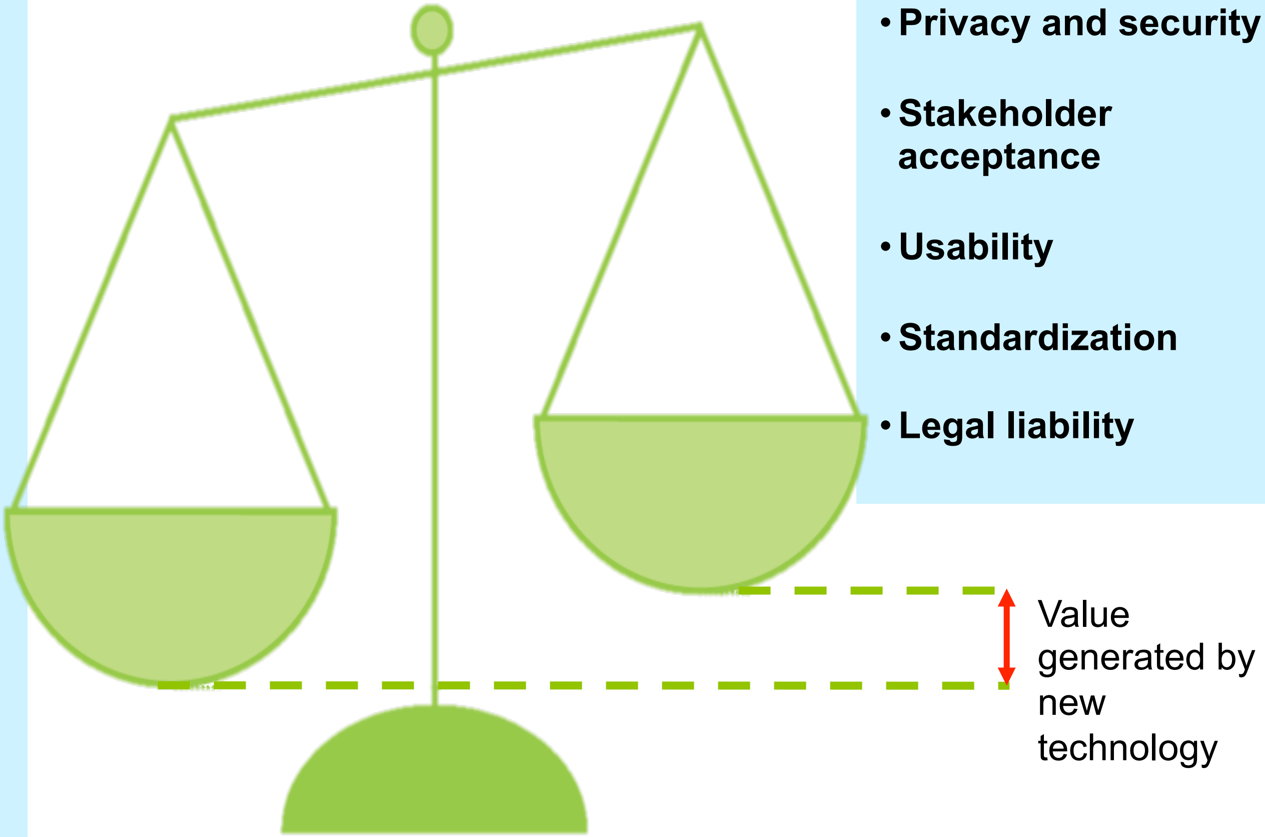
Weighing the risks

Benefits

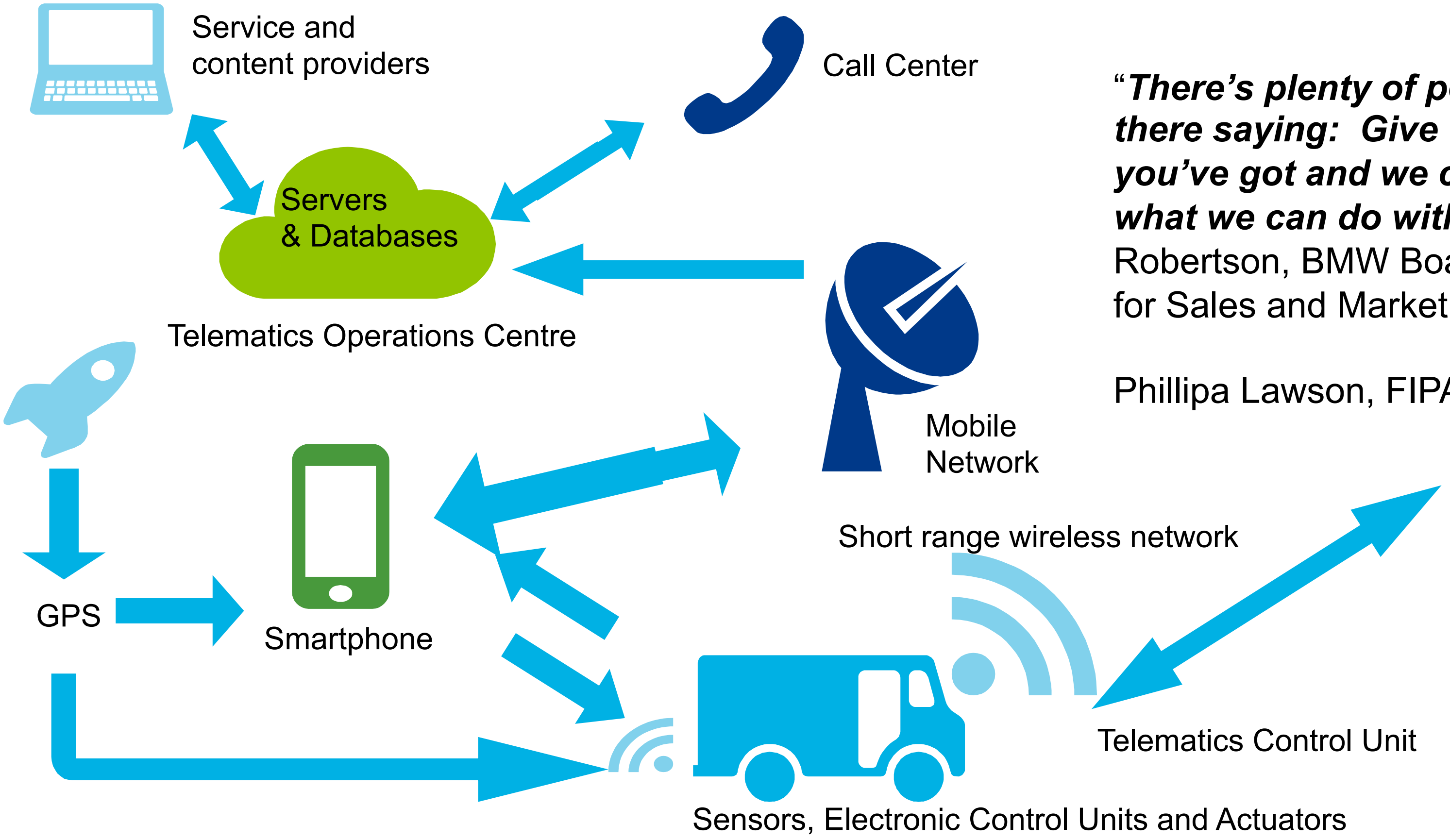
- **Increased profitability**
- **Enhanced customer experience**
- **Improved productivity**
- **Reduced costs**
- **Improved process**
- **Enhanced safety**
- **Increased efficiencies**

Risks

- **Privacy and security**
- **Stakeholder acceptance**
- **Usability**
- **Standardization**
- **Legal liability**



Connected car – Who is in the driver’s seat?



“***There’s plenty of people out there saying: Give us all the data you’ve got and we can tell you what we can do with it.***” Ian Robertson, BMW Board Member for Sales and Marketing

Phillipa Lawson, FIPA Report, 2015

What is being collected?

- Customer account data
- Vehicle performance data
- Driver behaviour data
- Biometrics and health data
- Location data
- Personal communications (voice, text, email, social networking)
- Web browsing data, stream audio or video content
- Personal contacts and schedules

Privacy Risks

Increased connectivity between devices and the Internet may create a number of security and privacy risks:

- Enabling unauthorized access and misuse of personal information
- Facilitating attacks on other systems
- Creating safety risks
- Lack of security in wearables when information is being transmitted
- Direct collection of sensitive personal information (geolocation, financial account information, health information, habits)
- The collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to make inferences or decisions a bout a person’s credit, insurance or employment

Internet of Things: Privacy & Security in a Connected World, Federal Trade Commission Report, January 2015

Risks – who owns the problem?

The legal risks:

- Property damage
- Multiple vendors
- Negligence
- Strict liability
- Warranty
- Fraud
- Product liability
- Privacy breach
- Misleading representations

The Players:

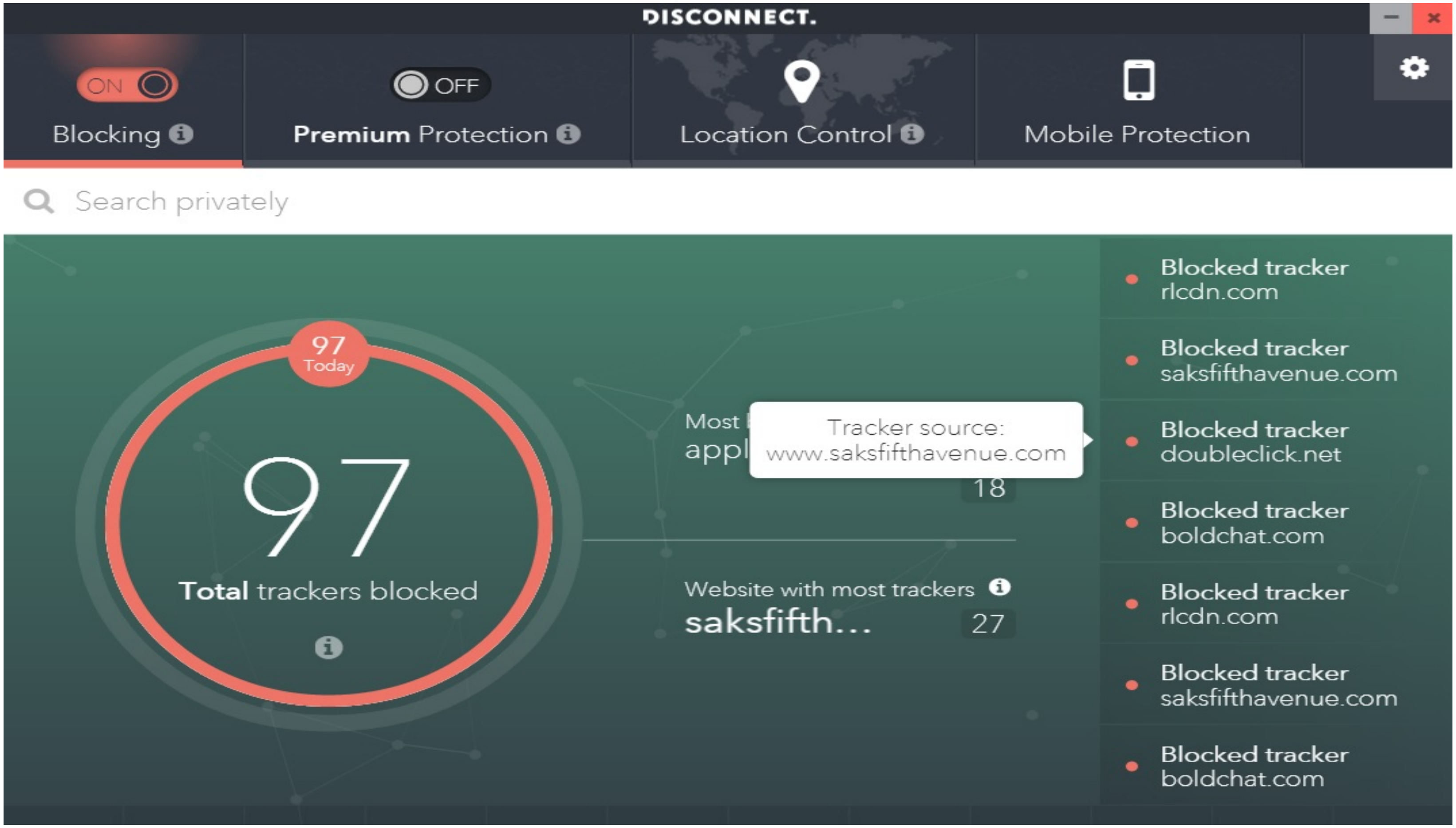
- Chip designers
- Art manufacturers
- Distribution retailers
- App developers
- Raw materials seller
- Product seller

Traditional approaches to privacy

- Notice/transparency
- Choice and control (opt-out)
- Use Limitation
- Responsible and ethical use of data
- Accountability
- Data Integrity

Tracking the Tracker

"If you're not paying for something, you're not the customer, you're the product being sold" – Andrew Lewis



97 Today

97 Total trackers blocked

Most … appl…

Tracker source:
www.saksfifthavenue.com

18

Website with most trackers
saksfifth… 27

Blocked tracker
rlcdn.com

Blocked tracker
saksfifthavenue.com

Blocked tracker
doubleclick.net

Blocked tracker
boldchat.com

Blocked tracker
rlcdn.com

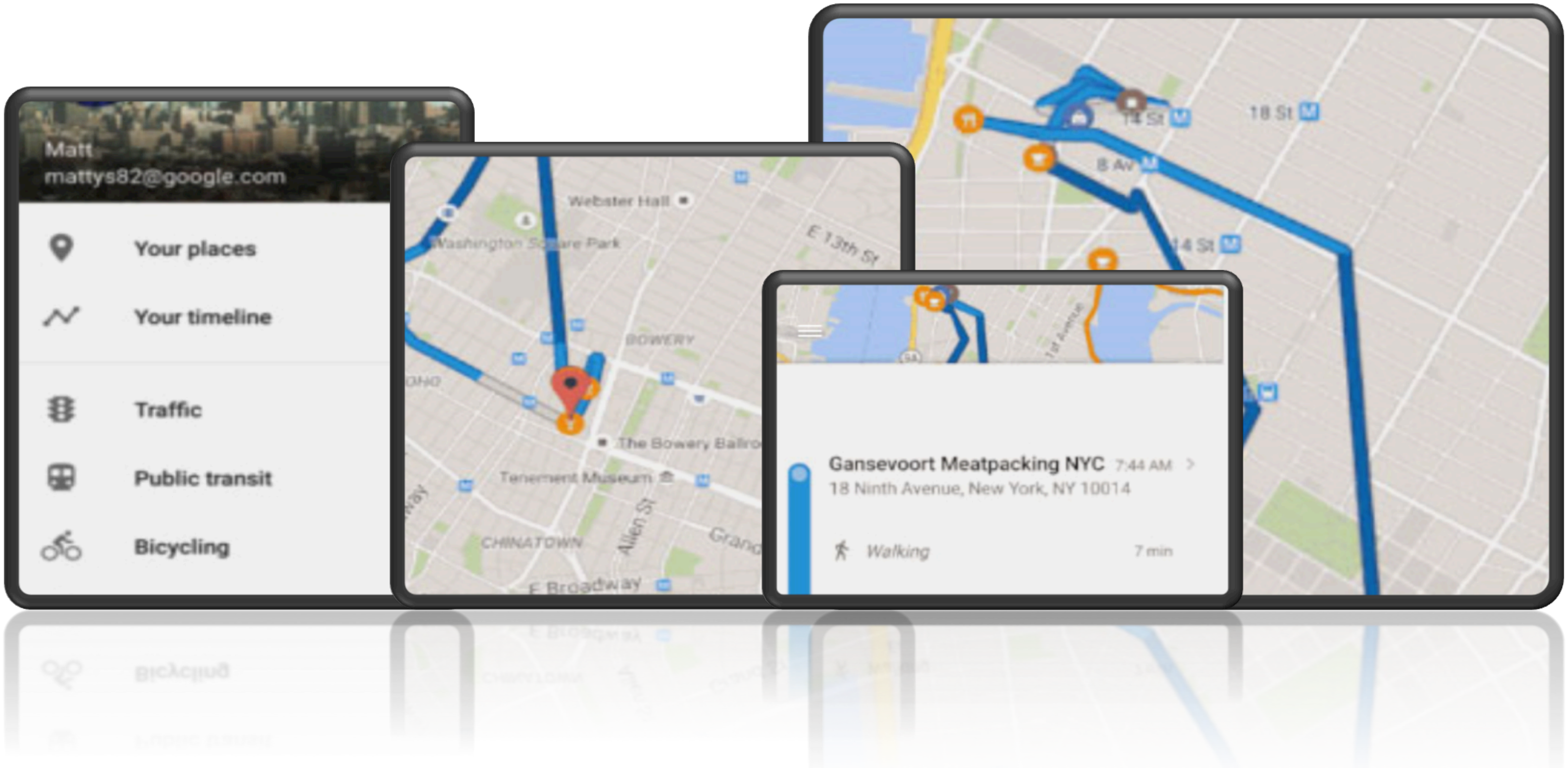
Blocked tracker
saksfifthavenue.com

Blocked tracker
boldchat.com

Saks fifth avenue was visited on both Internet Explorer and Google Chrome

How law enforcement can use Google Timeline to track your every move

"The expansion of Google's Timeline feature, launched in July 2015, allows investigators to request detailed information about where someone has been — down to the longitude and latitude — over the course of years."
– The Intercept, Jana Winter (November 6, 2015)

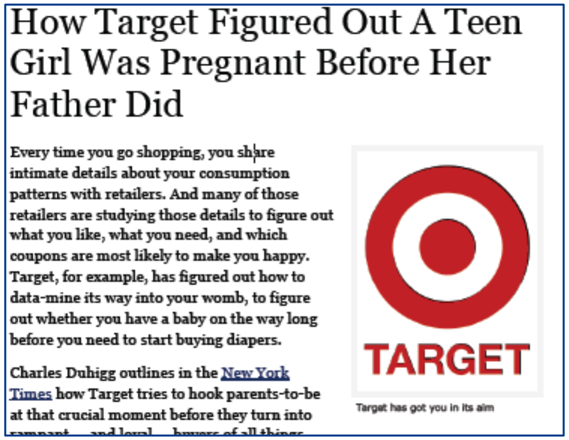


Gansevoort Meatpacking NYC 7:44 AM
18 Ninth Avenue, New York, NY 10014
Walking 7 min

Avoiding the “creep factor”

Understanding privacy risks at every stage of the connected digital consumer

Using analytics, Target Inc. took personally identifiable information and developed a list of 25 “indicator products” that could produce a “pregnancy prediction” for its female guests of childbearing age. The analytics findings enabled Target to estimate due dates in order to send coupons at specific stages of a woman’s pregnancy.



How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and loyal — buyers of all things

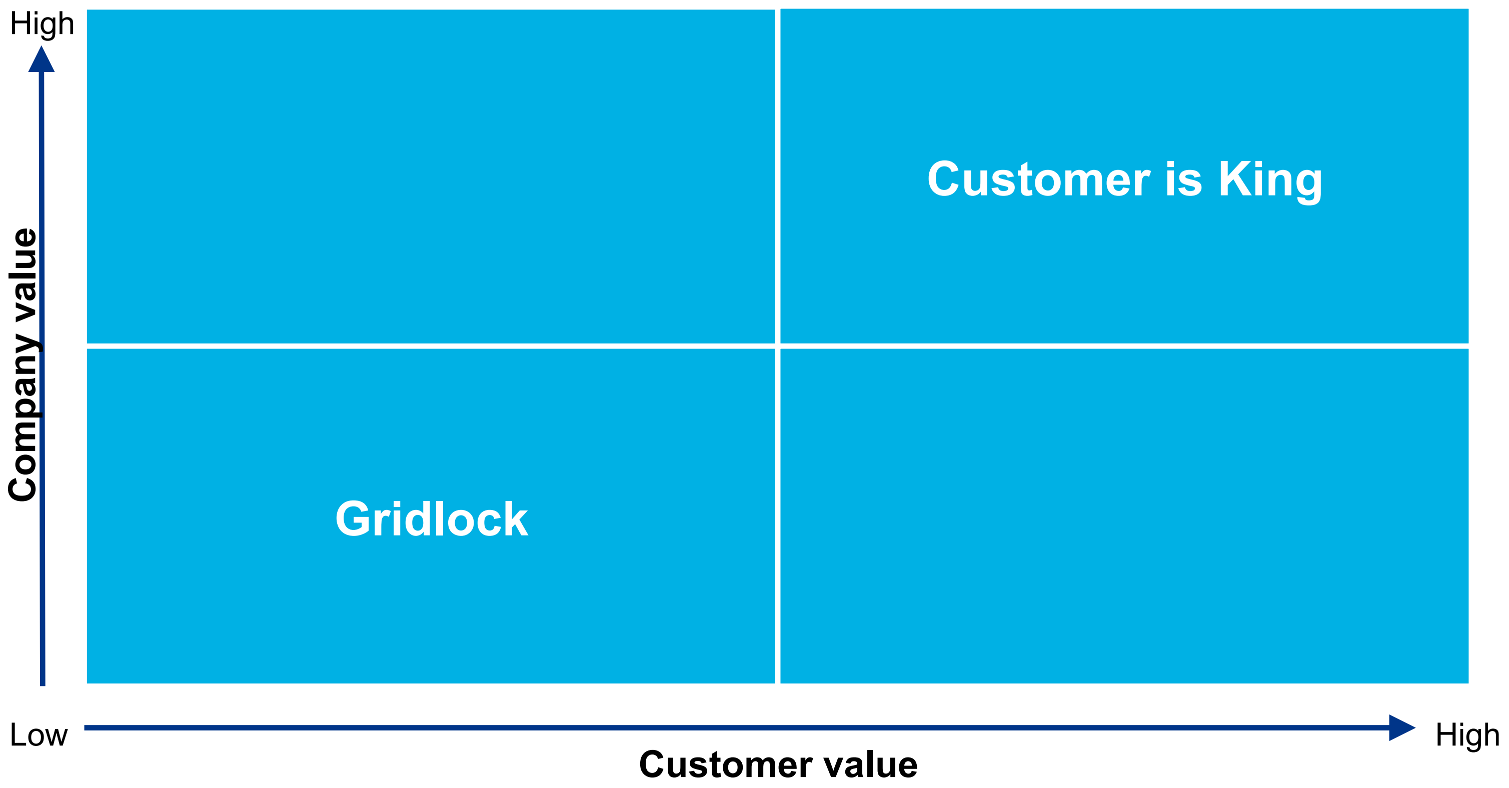
Target has got you in its aim

“I had a talk with my daughter” … “It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August….”

Privacy = Control

- User control is critical
- Freedom of choice
- Informational self-determination

Enabling privacy through trust results in a win-win scenario on the value grid

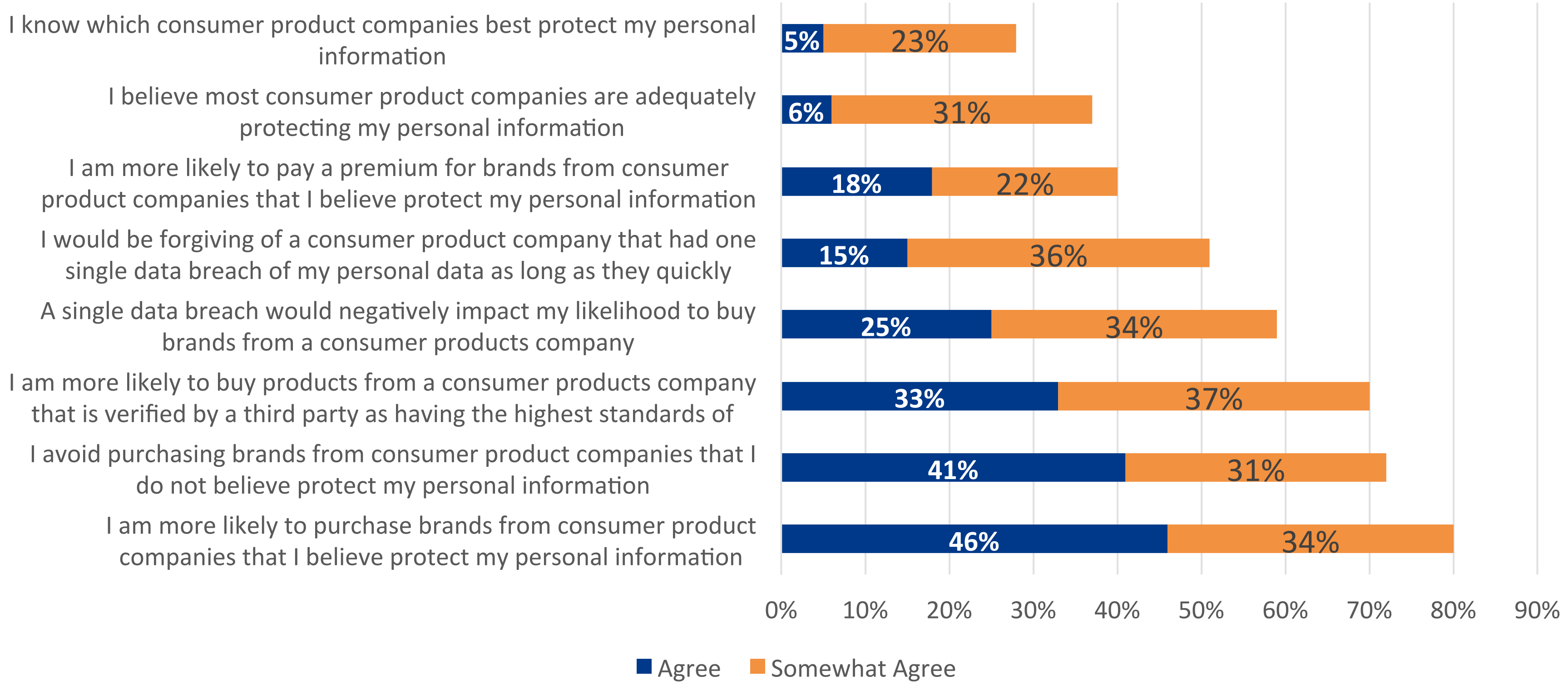


Customer is King

Gridlock

"We believe the customer should be in control of their information. You might like these so-called free services, but we don't think they're worth having your email, your search history and now even your family photos data mined and sold off for god knows what advertising purpose" – Tim Cook, Apple CEO at EPIC Conference

Consumers' attitudes and behaviours towards data privacy and security

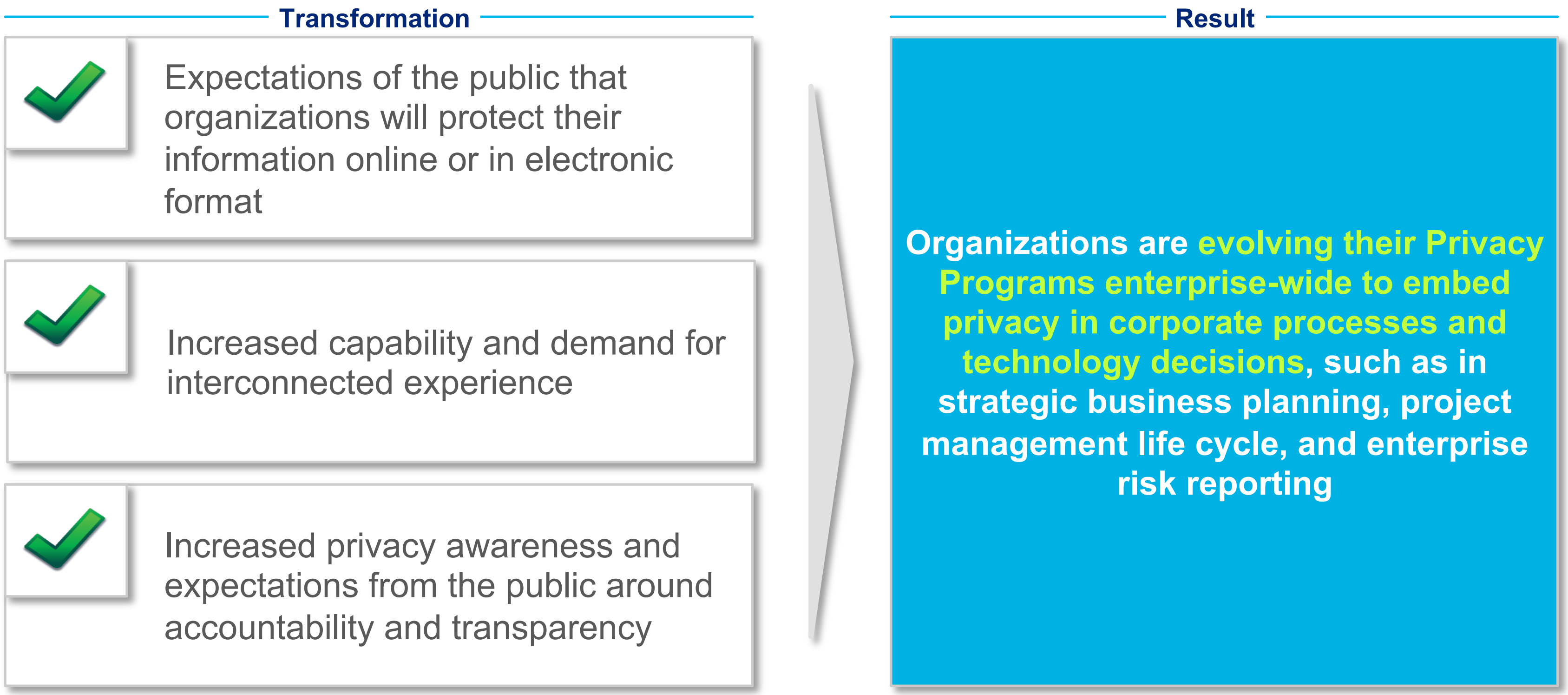


Source: Consumer responses from the product consumer and executive survey on data privacy and security – Deloitte LLP, August 2014

Market demand for privacy

Canadian privacy trends

Privacy programs are trending towards increasing oversight and advisory services to business unit/divisions on the privacy protections that our clients and the public expect.



Transformation

- ✓ Expectations of the public that organizations will protect their information online or in electronic format
- ✓ Increased capability and demand for interconnected experience
- ✓ Increased privacy awareness and expectations from the public around accountability and transparency

Result

Organizations are evolving their Privacy Programs enterprise-wide to embed privacy in corporate processes and technology decisions, such as in strategic business planning, project management life cycle, and enterprise risk reporting

Then and now – how organizations manage privacy

Privacy component	Past (late 90s to early/mid-2000s)	2010 onwards
Privacy driver	Legal compliance is a big privacy driver	Legal compliance *and* digital technologies are as much of a privacy driver
Incident reporting	Privacy incident monitoring and reporting processes are new – organizations are just drafting their breach response protocols	Mature privacy incident monitoring and reporting processes; more emphasis on streamlined communications and enterprise-wide training from incidents
Training	Privacy training likely to be general in nature and delivered "on paper" (e.g. Employees sign a generic "privacy pledge")	Privacy training likely to be customized to user groups and delivered in multiple formats (e.g. online, in-person, privacy reminders sent to users' smart phones)
Risk identification	General Counsel is responsible for privacy and is often the Chief Privacy Officer (CPO); CIO is responsible for data security; it is unclear who is primarily responsible for privacy and security risk identification and mitigation	LOBs, Marketing, IT/IM, Risk and IA also responsible for risk identification Privacy and security are more likely to be integrated within broader risk management plans

Emphasis on “accountability”

The Office of the Privacy Commissioner of Canada (OPC) and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia jointly issued regulatory guidance entitled *Getting Accountability Right with a Privacy Management Program*, which sets out detailed expectations for a comprehensive privacy management program. The guidance addresses the baseline fundamentals or “building blocks” of a Privacy Program and how to monitor it on an on-going basis:

Part A) Building Blocks		
Organizational commitment	**Buy-in from the top**	a) Senior Management **endorses the program controls**, and **monitors and reports to the Board**.
	Privacy Officer	b) Privacy should be seen as **improving processes, customer relationship management and reputation**.
	Privacy Office	c) Organization structure supports staff to monitor compliance and foster a culture of privacy.
	Reporting	**d) Internal reporting mechanisms** need to be established and **reflected in program controls.**
Program controls	Personal information inventory	a) Every organization needs to determine what personal information is held and where it is held.
	Policies	b) Organizations must develop and document internal policies that give effect to privacy principles established under Canadian privacy law.
	Risk assessment tools	**c) Conducting risk assessments, at least on an annual basis**, is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation.

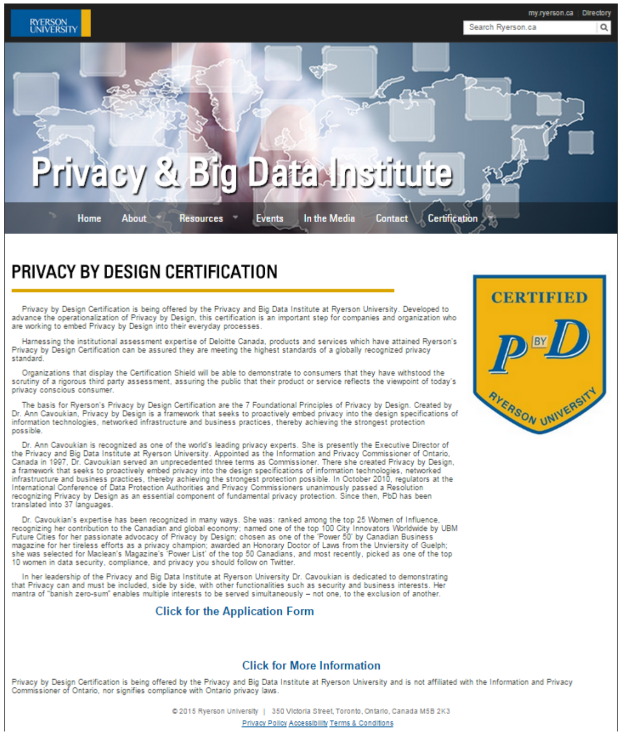
Part B) Ongoing Assessment and Revision		
Oversight and review plan	Develop an oversight and review plan	a) The Privacy Officer should develop an oversight and review plan on an annual basis for monitoring and assessing the organization’s privacy management program’s effectiveness.
Assess and revise program controls	**Treat risk assessment tools as evergreen**	b) The effectiveness of the Program should be monitored, periodically audited, and address the latest threats and risks, complaints or audit findings.

What is “Privacy by Design”?

Privacy by Design was created to reconcile the need for robust data protection with the desire for data-driven innovation.

Privacy by Design
The 7 foundational principles

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



PRIVACY BY DESIGN CERTIFICATION

Privacy by Design Certification is being offered by the Privacy and Big Data Institute at Ryerson University. Developed to advance the operationalization of Privacy by Design, this certification is an important step for companies and organization who are working to embed Privacy by Design into their everyday processes.

Harnessing the institutional assessment expertise of Deloitte Canada, products and services which have attained Ryerson's Privacy by Design Certification can be assured they are meeting the highest standards of a globally recognized privacy standard.

Organizations that display the Certification Shield will be able to demonstrate to consumers that they have withstood the scrutiny of a rigorous third party assessment, assuring the public that their product or service reflects the viewpoint of today's privacy conscious consumer.

The basis for Ryerson's Privacy by Design Certification are the 7 Foundational Principles of Privacy by Design. Created by Dr. Ann Cavoukian, Privacy by Design is a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible.

Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She is presently the Executive Director of the Privacy and Big Data Institute at Ryerson University. Appointed as the Information and Privacy Commissioner of Ontario, Canada in 1997, Dr. Cavoukian served an unprecedented three terms as Commissioner. There she created Privacy by Design, a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible. In October 2010, regulators at the International Conference of Data Protection Authorities and Privacy Commissioners unanimously passed a Resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. Since then, PbD has been translated into 37 languages.

Dr. Cavoukian's expertise has been recognized in many ways. She was: ranked among the top 25 Women of Influence, recognizing her contribution to the Canadian and global economy; named one of the top 100 City Innovators Worldwide by UBM Future Cities for her passionate advocacy of Privacy by Design; chosen as one of the 'Power 50' by Canadian Business magazine for her tireless efforts as a privacy champion; awarded an Honorary Doctor of Laws from the Unviersity of Guelph; she was selected for Maclean's Magazine's 'Power List' of the top 50 Canadians, and most recently, picked as one of the top 10 women in data security, compliance, and privacy you should follow on Twitter.

In her leadership of the Privacy and Big Data Institute at Ryerson University Dr. Cavoukian is dedicated to demonstrating that Privacy can and must be included, side by side, with other functionalities such as security and business interests. Her mantra of "banish zero-sum" enables multiple interests to be served simultaneously – not one, to the exclusion of another.

Click for the Application Form

Click for More Information

Privacy by Design Certification is being offered by the Privacy and Big Data Institute at Ryerson University and is not affiliated with the Information and Privacy Commissioner of Ontario, nor signifies compliance with Ontario privacy laws.

© 2015 Ryerson University | 350 Victoria Street, Toronto, Ontario, Canada M5B 2K3

Privacy Policy Accessibility Terms & Conditions

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

Operationalizing Privacy by Design
Privacy controls framework

- The privacy controls framework is organized around the 7 Privacy by Design principles. Each principle is framed by a set of privacy criteria and illustrative privacy and security controls:

  http://ryerson.ca/content/dam/pbdi/Certification/Privacy%20by%20Design%20Certification%20Program%20Assessment_Privacy%20Controls%20Framework%2020150716.pdf

Principle	Assessment criteria	Illustrative controls
Principle 1	1-7	1-18
Principle 2	8-11	19-32
Principle 3	12-14	33-38
Principle 4	15	39-42
Principle 5	16-24	43-89
Principle 6	25-26	90-94
Principle 7	27-30	95-107
Total	**30 criteria**	**107 controls**

Objective and measurable assessment criteria

Our Privacy by Design control framework is based on a set of well-defined privacy criteria and controls that align to the 7 foundational principles:

Principle 1: Proactive not reactive; preventative not remedial

Assessment criteria	Illustrative control activities
1.1 Privacy risk management plan A risk assessment strategy and process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.	**1.1.1 Privacy risk assessment process** • A process is in place to periodically assess the organization’s privacy practices, identify the risks to the organization’s personal information and implement mitigating controls. • Such risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as emailing unprotected sensitive information). When new or changed risks are identified, the privacy risk assessment and the response strategies are updated. The process tracks the implementation of mitigating and corrective actions and re-evaluates practices and risks in a closed loop fashion.
	1.1.2 Integration with privacy breach management, complaint resolution and monitoring • The process considers factors, such as experience with privacy incident management, the complaint and dispute resolution process, and monitoring activities.

Contextually appropriate data practices

Design choices

Build privacy and security into devices at the outset, rather than as an afterthought – into every stage of development even the design cycle

- Management portals or dashboards
- Icons
- “Out of Band” communications requested by consumers
- General privacy menus
- A user experience approach
- Choices at point of sale
- Tutorials
- Codes on the device
- Choices during set-up

Early adopters

CANATICS
Canadian National Insurance Crime Services

PHEMI
HEALTH SYSTEMS

Myth #1 Believing that privacy is really the CPO’s problem

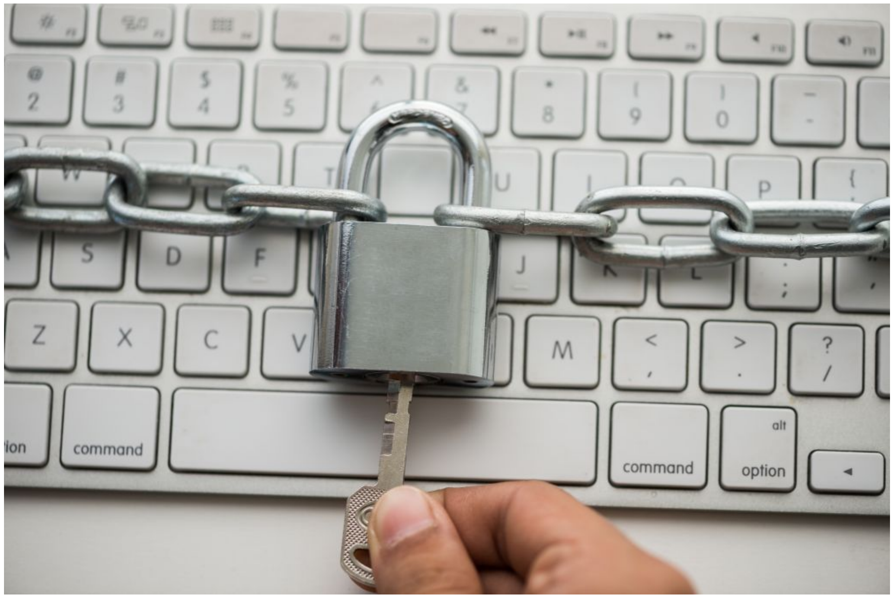
- Don’t assume that your project has no privacy implications... And even if it does, don’t assume that the CPO or his or her team will cover off privacy
- Believing there will be no privacy show-stoppers because the CPO is involved is common but potentially risky
- Don’t assume the CPO has a deep understanding of your project

#1

Believing that privacy is really the CPO's problem

Break the silos

- Everyone working for an organization that depends on personal information is in it together
- Formally document roles, responsibilities and accountability so they are clear:
  - Across departments
    - Define risk ownership
    - Identify and assess interdivisional reliances
    - Formalize data governance



Myth #2 Worrying only about legal compliance

- Privacy is really a legal problem
- Limited or no linkage to business strategy and organizational objectives
- Does not consider risk taking as a means to value creation
- Weak connection to risk appetite

#2

Worrying only about legal compliance

Treat privacy as a strategic business advantage

- Integrate privacy risk management into strategic planning and resource allocation
- Analyze privacy risk and return tradeoff
- Don’t leave privacy as an afterthought – build protections into new technologies upfront

Digital progress

Then and now…

1957:

2017:

13 men delivering a computer…

A person may wear 13 computing devices…

For more information….

Sylvia Kingsmill, BA, LLB
National Partner
Data Protection and Digital Privacy Leader
skingsmill@deloitte.ca
416.643.8238

Deloitte.

The information contained herein is not intended to substitute for competent professional advice.