Freedom and Control: Engineering a New Paradigm for the Digital World

May 8, 2014

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

Dan Kruger
President and CEO
Absio Corporation

Absio®
Take Control of Your Digital World℠

Freedom and Control: Engineering a New Paradigm for the Digital World

TABLE OF CONTENTS

Introduction 1
Preface 2
Part 1: Demystification 3
- Control and Freedom 3
- Two Worlds 3
- Seven Problems 4
  - 1. The Foolish Object Problem 4
  - 2. The Sporadic Control Problem 4
  - 3. The Object Evaluation Problem 5
  - 4. The Authentication Problem 5
  - 5. The Unaccountable Pseudonym Problem 5
  - 6. The Administrator/Data Separation Problem 5
  - 7. The Complex Administration Problem 5

Part 2: Control Engineering 6
- Engineering Intelligent Digital Objects 6
- Intelligent Digital Object Agent 7
- Digital Object Management Ecosystem 8
- Solving the Seven Problems 9
  - 1(a) Foolish Objects 9
  - 2(a) Sporadic Control 9
  - 3(a) Object Evaluation 9
  - 4(a) Authentication 9
  - 5(a) Unaccountable Pseudonyms 9
  - 6(a) Administrators and Data Separation 10
  - 7(a) Complex Administration 10

Part 3: Conclusion 11
References / Additional Reading 12

Today, every discussion about changes in technology, business and society must begin with data. In its exponentially increasing volume, velocity and variety, data is becoming a new natural resource. It promises to be for the 21st century what steam power was for the 18th, electricity for the 19th, and hydrocarbons for the 20th.

2012 IBM Annual Report, Data Strategy

Introduction

Individuals are losing effective control over their personal information in this era of ubiquitous social, mobile, and cloud computing. In the emerging "Internet of Everything" world, proponents of Big Data analytics promise new insights, innovations, and benefits, from real-time tracking of flu epidemics and traffic flows, to enhanced personalization, convenience and efficiencies, to identifying terrorists and enhancing public safety.

Some are saying that traditional Fair Information Practice Principles (FIPPs) and privacy laws present barriers to the new reality and imperative of big data, and must give way. Our data is out there, the genie is out of the bottle, they say, and so let's face the facts. This being the case, why not dispense with informed consent of individuals? Why not reduce or eliminate restrictions on obtaining the personal data collection, use and retention altogether, and focus instead on defining socially acceptable and unacceptable uses of personal data, while stepping up accountability and enforcement efforts? In the words of a leading proponent of this view, Viktor Mayer-Schönberger, "Informational self-determination has turned into a formality devoid of meaning and import." (We couldn't disagree more!)

There are, many downsides to the above. Asymmetries of information typically heighten power imbalances and put individuals at a distinct disadvantage. Consequently, individuals will suffer unwanted surveillance and profiling, become victims of incorrect inferences growing, false positives, and other automated decisions, be subjected to manipulation, social controls, reduced choices, discrimination, unwanted exposure, lost employment, insurance and travel opportunities, become victims of unknown and unaccountable misuses and abuses involving their personal data, as well as victims of identity fraud and theft.

We described in our 2008 *Privacy in the Clouds* paper with IBM an emerging world of networked data transactions that involve the individual less and less directly, rendering the client-server model of online transactions increasingly obsolete, and with it, the traditional concept of informed consent and informational self-determination problematic. In that paper we called for greater research, innovation and development of trusted privacy-enhancing technologies in the service of individuals, not corporations or governments. We anticipated four areas that could allow individuals to extend and maintain control over their personally identifiable data. These included technologies to: (1) enable personal data itself to become "smarter" and more context-aware; (2) ensure more secure and trusted personal devices to act as intermediaries and servants; (3) develop

trusted agents in the cloud, capable of brokering and monitoring transactions on behalf of the individual; and (4) create a class of third party services, held to the highest standards of accountability and trust.

The future of privacy will not be assured by **weakening** traditional fair information practice principles that underpin individual privacy rights. Rather it will only be through a redoubling of efforts, bold innovations and robust implementation of new and exciting technology-assisted models that an individual's capabilities will be extended and freedom assured.

In the context of this discussion paper, we are emphasizing in particular principle 7 of the *7 Privacy by Design* Foundational Principles — "Keep it User-Centric." As a counterpoint to those calling for the world of tomorrow to be less user-centric, since 2008 we have been writing about evolutionary forms of "SmartData" that are able to understand, embed, express, and enforce individual preferences directly into personal data. (Tomko, 2008; Tomko et al, 2012; IPSI SmartData Symposium 2012). The emergence of a personal data ecosystem that puts individuals squarely in the center of cloud-based agent-assisted data transactions and repositories is a clear example of robust application of the user-centric principle (Cavoukian and Reed 2012; Cavoukian, 2013).

Now, with the help of Absio, we are setting out a vision of the architectural and engineering requirements needed to bring about a truly user-centric Internet — one that involves fusing together data-centric approaches with trusted personal devices, agents, and third-party services.

Preface

Privacy and cybersecurity professionals, creators of digital property, and countless policy-makers have spent decades fighting to civilize the digital world, but they have lacked the most fundamental tool they need to succeed, namely — information systems engineering that enables true control of digital data.

It is now possible to change the paradigm of the digital world from "Use At Your Own Risk," to "My Data, My Rules." Imagine such a world, if you can!

Too many individuals and organizations are resigned to large-scale computer-based surveillance, invasion, and expropriation. The purpose of this paper is to explain, in plain language, why we believe that resignation to be unwarranted.

Part 1: Demystification

Control and Freedom

Instituting a significant degree of control over who can interact with us, what people and institutions know about us, and the use and value of our property is essential for establishing and maintaining freedom.

If too many of our relationships are involuntary, if we cannot determine if and when we should reasonably identify ourselves in public and if we have no control of our own property, then we are not free.

In the digital world, as in the analog world, the problems of control and freedom are inseparable.

Two Worlds

The analog world is comprised of the objects that we can see, feel, touch, and experience. Our observations guide our perceptions and actions.

In the last 30 years we created a new set of problems by engineering a world we cannot see, yet are utterly dependent on — the quantum-scale word of digital data.

Unlike the analog world that we directly perceive and manage, we cannot access the digital world without tools. Our tools must enable us to accurately perceive and effectively manage the digital world, utilizing our analog senses and perceptions.

In many cases we deal with digital communication and information as if it is part of a completely different universe, when in fact it is amenable to the same constraints as analog communication and information.

To clarify:

- Every form of communication and information in the digital world is based on an analog world counterpart. Email equates to written correspondence, the Internet acts as a transportation system, etc.
- The digital world is comprised of computers, software, and networks that manufacture, transport, and manage *digital objects* — bundles of zeroes and ones that contain all digital data.
- Digital objects are much smaller, lighter, faster, and less energy-intensive to manufacture and transport than their analog world counterparts. This is why the digital world was built.
- Digital objects are entirely physical, but only at the quantum scale. They have structure, form, and persistence. If their physical substrate is sufficiently disturbed or destroyed, the digital objects and the information they contain vanish.
- The digital world is the product of science and engineering. If we want to change its behaviour, we have to change some aspect of the way it is engineered. We do this constantly.

- Digital objects carry the data needed for every function of the digital world. They carry information, direct communication, establish identity, and encapsulate property.
- We exercise control in the digital world by exercising control of digital objects.
- With the proper engineering, control of digital objects can be as manageable as control of their analog counterparts.

Seven Problems

In order to control digital objects, we must overcome seven problems.

1. The Foolish Object Problem

The digital objects manufactured by current systems are "foolish." That may sound strange, but it appears as the root of all the problems we address in this paper.

Foolish objects give up their information payload to any system that asks for it, they do not know where they are or where they have been, do not know who created them, and do not know how to call home, or who has changed them, or what was changed. In this sense, we consider them to be "foolish."

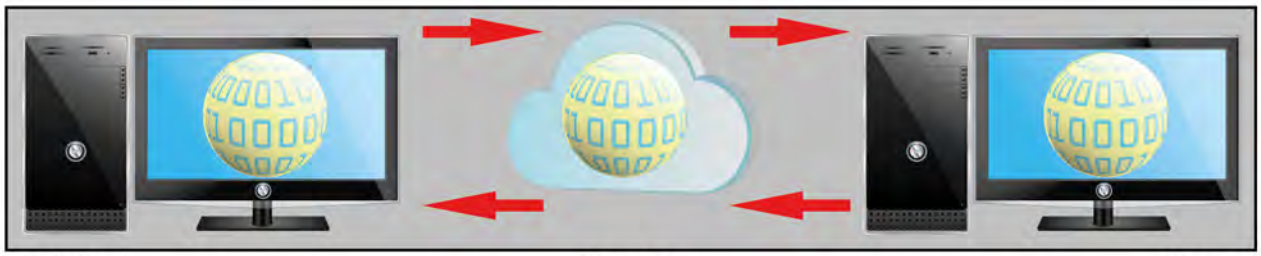
Alarmingly, the vast majority of our digital assets are stored in objects that behave as fools, in an adverse environment.

2. The Sporadic Control Problem

Digital objects are the most easily copied and transported objects that mankind has ever created. Digital objects proliferate at an immense rate because computers are in essence, digital-object copy machines attached to a global shipping and receiving service known as the Internet.

Our current notions of digital control are based on a historical mindset that is no longer sufficient — perimeter security. In the early days of computing, people could not get into the building containing the computer or carry bulky physical media out of the building without permission and witnesses to these acts. Perimeter security, by itself, provided a reasonable degree of control.

In a networked world, perimeter security may provide the occasional containment of the copies of some digital objects, some of the time. But by itself, it gives us only sporadic control. Sporadic control is tantamount to no control — it's not good enough.



3. The Object Evaluation Problem

Just as we send digital objects to other computers, we also receive digital objects from other computers. We currently have little ability to evaluate the objects that we receive. We do not know, with any significant degree of certainty, who sent them, why they were sent, or what they can do. Unevaluated objects open us up to everything from spam, to tracking cookies, to malware.

4. The Authentication Problem

We cannot be certain that the person who we think is using a computer is actually the one using it to send or receive information. Username and password authentication is very weak and is, after the foolish object problem, the most significant contributor to the lack of control.

5. The Unaccountable Pseudonym Problem

When people are free to use public digital pseudonyms that are not authoritatively tied to their true name, bad actors are free to engage in bad acts, with very little chance of being held accountable for their actions.

Far more important, legitimate people engaged in legitimate activities are not able to present known legitimate pseudonyms in the digital public arena. Unlike the analog world, individuals in the digital world are not free to withhold their identity when asking for directions, shopping, attending a political event, or any other of the myriad everyday activities they do, without being required to identify themselves.

6. The Administrator/Data Separation Problem

In almost all current systems, the ability to administer a body of digital objects inherently provides the administrator access to the information payloads of those digital objects. Many of the largest and most costly data breaches arose as a direct result of this problem. Access to data must be separated from the ability to organize and manage data.

7. The Complex Administration Problem

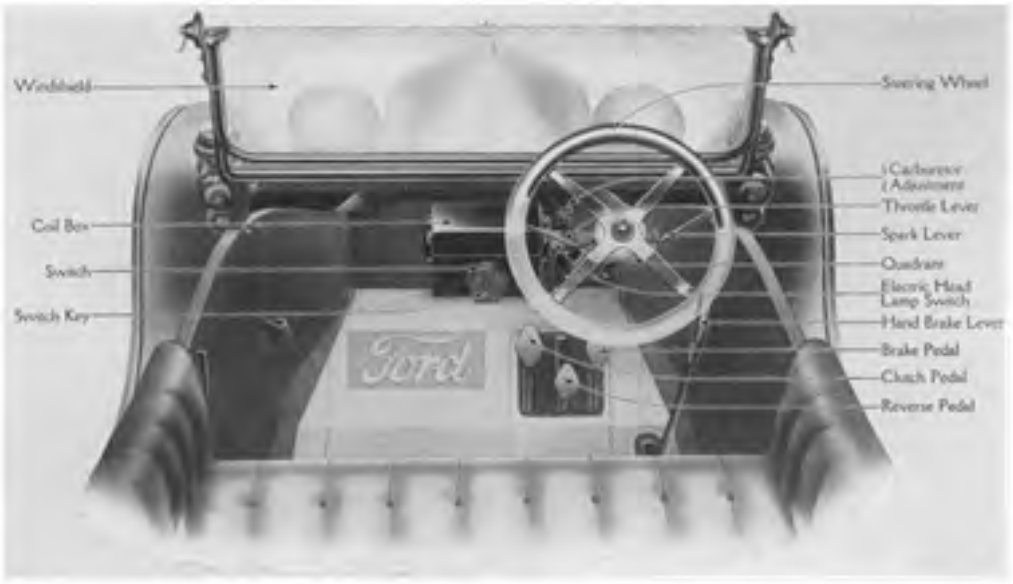
Currently, administering notification and consent is far too complex. This gives rise to the paternalistic argument that individuals are unable to be responsible for and preserve the privacy of their communications, records, and property.

That argument is wholly based on the specious assertion that the way we currently manufacture and manage digital objects is the only way that they can be manufactured and managed. It is delightfully reminiscent of the arguments advanced years ago by the telegraph industry advanced against the telephone industry. The telegraph companies claimed that telephones were merely a novelty and that people couldn't manage their communications for themselves as well as the telegraph company could. Some aspects of human behaviour never change!

Part 2: Control Engineering

Control engineering for the digital world has the same goal as control engineering in the analog world: to build sufficient intelligence and reliability in engineering controls so that the system may be dependably administered by the average person.

For example, the engineering controls for using the brakes on the early Ford Model T were by modern standards, neither intelligent nor reliable. The braking administrator (the driver) had to:



1) Retard the hand throttle, then

2) Retard the spark (a different hand control), then

3) Pull the handbrake, (yet another hand control), then

4) Put the car into reverse (operate three foot pedals which required both feet), then

5) Press the foot brake, all in the right order, and as rapidly as possible to stop the car.

Today, all we need to do is to step off the gas pedal and step on to the brake — two controls, one foot. Improved engineering controls have made such administration easy and reliable.

Engineering Intelligent Digital Objects

The goal of making digital objects easy to manage by ordinary people yields a clear and implementable set of engineering and economic requirements.

From an engineering standpoint, the system must be able to:

- Create intelligent objects, not foolish ones;
- Turn existing foolish objects into intelligent objects;
- Manage intelligent objects across the various systems that host them;
- Transmit the intelligence in the objects to software applications;
- Receive intelligence from software applications and store it in intelligent objects.

From an economic standpoint, the system must be able to:

- Improve control of digital data;
- Make administration simpler and more reliable;
- Produce a significantly better ROI than current security engineering, which has long since passed the point of diminishing returns.

To transform a foolish object into an intelligent object, a system must be engineered to:

- Encode the object so that it is undecipherable, by default. In the analog world, the ability to withhold information is a precondition for granting permission to use it. If you can't withhold information, permissions are meaningless. This must also be the case in the digital world.
- Enable the object to contain any data format.
- Separate control instructions from the object's information payload so that control instructions govern access to the information payload and usage of the information payload after it is accessed.
- Provide a control information architecture that comprehends object-identifying information, who-what-when-where usage history, and metadata that supports data organization, discovery and accountable pseudonymity.

Intelligent Digital Object Agent

Intelligent objects can be managed by an Intelligent Digital Object Agent(Agent) — a software application that can be installed on existing computers and integrated with existing and new software applications.

An Agent is inserted between an application and the operating system that hosts it. By interposing itself between an application and the operating system, the Agent intercepts foolish objects created by the application and transforms them into intelligent objects.

When an Agent opens an intelligent object, it evaluates the control information and passes behavioural instructions, along with the appropriate portion of the information payload to an Agent-compliant application. It also receives information from the Agent-compliant application that supports versioning, audit, provenance, and usage control.

Digital Object Management Ecosystem

Intelligent Objects and Agents must be implemented in a way that supports the development of a Digital Object Management Ecosystem.

The term ecosystem here connotes the establishment of a profitable marketplace for intelligent digital objects and applications. Establishing a new and powerful set of profit opportunities, supported by intelligent regulation, is the surest and quickest way to enable ordinary people and organizations to gain control of their digital world.

The Agent provides the basis of the ecosystem and must be made available for multiple operating systems, with a full set of tools for developers. Agent-compliant applications generate intelligent digital objects, giving users control of their digital data everywhere it may be located — on their devices, in the cloud, while in transit, or on someone else's device.

Authentication and private encryption keys are managed by an Agent on each individual user device. The transfer of data to and from other users is entirely permission-based. Users establish the policies, why the applications in the ecosystem enforce them. This puts users in control of their digital identities and interactions.

In order to support this ecosystem, there must be a service provider (General Service Provider or GSP for purposes of this paper) that acts as an authoritative registrar and provides directory services for individuals and product/ service providers. The GSP must enable registrants to publish information in a public directory, with options to include as little or as much identifying information as the user desires. Third-party attestation of a registrant's identity may be added, at the discretion of the user, to facilitate greater trust in the communications.

The GSP must also provide normal business services, such as cloud storage, directly and through a registered third party.

The GSP must be able to support the federation of public identities with private entities within private service providers (PSPs). PSP's, usually organizations and governments, must be able to build their own private control ecosystems. Control becomes ubiquitous when there is an ecosystem of ecosystems.

The GSP is necessary to support the control ecosystem, but CANNOT — have the ability to decipher intelligent objects anywhere in the ecosystem not in cloud storage, not in transmission, not on devices, and not in federated systems. "Cannot" is very different from will not. In order to provide true privacy and control, the GSP cannot have the means to decipher the —intelligent objects it stores and transmits for the public or provide others with a means to do so, even if subverted or ordered to provide access. The ability of the GSP to decipher the intelligent objects it holds must be — and has been — engineered out of the system. PSPs are different in that they can and should have the ability to decipher their registrants' data. In PSPs, the data belongs to the PSP, not to the registrants.

The only data the GSP must be able to deliver, when legally required, is the true name of the general public registrant and pseudonyms used by that registrant.

Law enforcement and national intelligence operations, when following proper warranted procedures, and on an individual basis, should be able connect a pseudonym to a true name.

Solving the Seven Problems

1(a) Foolish Objects

There is no reason why foolish objects cannot be engineered to be intelligent by default. The ecosystems of Intelligent Objects, Agents, Agent-Compliant Applications, GSPs, and PSPs enable the persistent control of intelligent, digital objects, anywhere they may be, all the time. It is important to note that creating intelligent, controlled digital objects does not solve the analog problem. When digital information is converted to analog information, people can, and will, abuse it. We have been managing this issue since the advent of written language. However, through proper system engineering we can successfully thwart the large-scale ubiquitous loss of information control that we are currently experiencing in the digital world.

2(a) Sporadic Control

Perimeter security alone no longer provides sufficient protection for our data. By building control into the data itself, we can protect information no matter where it travels. Preventing loss of control by mere physical copying or interception makes the job of the hacker much more difficult. Products and processes that prevent the installation or operation of malware are rapidly gaining traction in the marketplace. Combining them with intelligent digital objects helps to thwart attacks on data in storage, in movement, and in memory.

Providing a common control technology to developers greatly simplifies their need to create a control system (most developers do not like and are not good at that type of engineering), or to figure out how to accommodate multiple control systems — the current Tower of Babel they have to deal with. As more applications use an Agent, control will become much more consistent.

3(a) Object Evaluation

Intelligent objects are more easily evaluated than foolish objects, and just as importantly, malicious intelligent objects (such as malware encapsulated in an intelligent object) are more traceable to their originators. Malware that can be tied to its publisher takes all the fun out of malware. Radically increasing the difficulty, cost, and risk of large-scale data theft is within our reach.

4(a) Authentication

Freedom and control begin by enabling users to proactively choose their interactions, rather than simply react to unsolicited contact. When users can decide whether or not they trust any given identity, the authentication problem is greatly diminished. There are a number of enhanced authentication mechanisms now available, such as biometric authentication, for those seeking to establish a greater level of trust.

5(a) Unaccountable Pseudonyms

Anonymity alone does not provide privacy. Without accountability, anonymity and pseudonymity can be misused to compromise the privacy of others. In a Digital Object Management Ecosystem, the GSP does not allow pseudonyms that are disconnected from true identities. Increasing the strength of an identity is

an economic advantage for legitimate users doing legitimate things. Bad actors will find the use of the intelligent object ecosystem inhospitable — their interest being in anonymity associated with a lack of accountability, not privacy.

6(a) Administrators and Data Separation

When control is built into intelligent objects, it is straightforward to separate management rights from information payloads based on permissions granted by the custodian of the data. This allows administrators to organize and distribute content as needed without directly gaining access to the information. The intelligent object ecosystem enables the creation of personal software agents that find and deliver information with more precision, less effort, and without loss of privacy.

7(a) Complex Administration

Shifting policy enforcement from people to applications reduces workload and the opportunity for mistakes, especially in complex security environments. The impact of automation in this arena will produce a degree of control and safety not currently available. In a Digital Object Management Ecosystem people set the policies — they are embedded in the data; compliant applications have no choice but to follow them, while non-compliant applications will not be able to read them.

Part 3: Conclusion

The Digital Object Management Ecosystem is now possible due to the same reason as every other major change in the last 30 years: increased processing power.

Increased processing power enabled the change from character interfaces to graphical user interfaces. Software that used to require specialized expertise to operate gave way to applications that virtually anyone can use, because developers used increased processing power to build more intelligence into the applications. Finding, ordering, and shipping a product across the country used to be a major undertaking — abundant processing power at the edge and in the cloud now makes that trivial from the standpoint of the user.

Desktops shrank to laptops and then to smartphones and tablets. It used to take elaborate planning to get work done on the move; now it is a matter of course. All of that simplification is a result of innovative software engineers harnessing increased processing power.

From the standpoint of the ecosystem, what we now address as separate issues of privacy, data security, and property preservation are aspects of control that differ only in the selection of which digital objects are being made intelligent.

Market demand for control is high and increasing daily. It is being driven by governments, businesses, legislators, regulators, insurers, and above all, the powerful human desire for freedom, autonomy, and privacy. Smart software and service providers will take advantage of the disruption intelligent digital objects bring to increase revenue, market share, and profits, by delivering whatever aspect of control their customers want.

In 2008, *Privacy by Design* leadership identified four innovations that could allow individuals to extend and maintain control over their data. These included technologies to: (1) enable personal data itself to become “smarter” and more context-aware; (2) ensure more secure and trusted personal devices to act as intermediaries and servants; (3) develop trusted agents in the cloud, capable of brokering and monitoring transactions on behalf of the individual; and (4) create a class of third party services held to the highest standards of accountability and trust.

An intelligent digital object ecosystem meets all of these requirements.

We have witnessed three great waves of change in the digital world since the mid-1980s. First came personal computing. Then came the commercialization of the Internet in the mid-1990s, giving us connected computing. Then roughly ten years ago, mobile computing exploded on the scene.

The next great wave, just now beginning, is controlled computing — we will be able to keep all of the gains of the last 30 years — but now, we can reclaim our freedom — our privacy, through personal control.

References / Additional Reading

Absio Corporation www.absio.com:

_____ Cyber Sanity at: http://bit.ly/RPqgOh

_____ Gaining Control of Our Data at: http://bit.ly/1l8Qo0S

Absio blog (Dan Kruger) at: http://absio.com/blog

Ann Cavoukian.

(2012) *Privacy by Design and the Emerging Personal Data Ecosystem* at: http://bit.ly/1mEKKmI

(2010) *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, at: http://bit.ly/1tHHv2c

(2008) *Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet*, at http://bit.ly/R82r3p

Ann Cavoukian and Drummond Reed. (2013) Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design, at: http://bit.ly/1lJWkQC

Ann Cavoukian, Alexander Dix, and Khaled El Emam. (2014) *The Unintended Consequences of Privacy Paternalism*, at: http://bit.ly/1nsv0py
Press Release: Paternalistic Approach to Privacy Will Deliver Unintended Consequences, at: http://bit.ly/1fbmngJ

IBM (2013) Annual Report – Data Strategy
www.ibm.com/annualreport/2013/strategy-data.html

IPSI SmartData International Symposium: Privacy Meets Evolutionary Robotics: Protecting Our Freedoms With Virtual Tools, University of Toronto, Canada (14-16 May 2012) proceedings at: www.ipsi.utoronto.ca/sdis/index.html

Privacy by Design: www.privacybydesign.ca

George Tomko. (2008) *How to Preserve Freedom and Liberty: Design Intelligent Agents to be Smart and Respectful of Privacy*, at http://bit.ly/QC5RLv

George J. Tomko, Hon Kwan, and Don Borrett. (2012) *SmartData: The Need, the Goal, the Challenge* (2012) at: http://bit.ly/1lJWac0

About the Authors

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner, Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to proactively embed privacy into the design specifications of information technology and accountable business practices, thereby achieving the strongest protection possible. In October 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection. This was followed by the U.S. Federal Trade Commission's inclusion of *Privacy by Design* as one of its three recommended practices for protecting online privacy – a major validation of its significance.

An avowed believer in the role that technology can play in the protection of privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in numerous international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening consumer confidence and trust in emerging technology applications.

Dan Kruger
President and CEO, Absio Corporation

Dan Kruger is founder, President and Chairman of the Board of Directors of Absio Corporation, based in Highlands Ranch, Colorado, a position he has held since 2009. A pioneer in software-enabled collaboration, Dan is a 30-year veteran consultant to businesses on teamwork, communication, technology strategy and the design and application of collaboration software.

In 2002, Dan founded Workplace Architects, the leading provider of drag, drop and configure application development Web parts for Microsoft SharePoint. He later sold Workplace Architects to Quest Software (now owned by Dell Inc.) and managed the product globally. Dan was also founding CEO of Construction News Service (now iSqFt), a leading software-as-a-service company serving the commercial construction industry by offering its subscribers access to a network that connects tens of thousands of general contractors, subcontractors, suppliers and manufacturers. iSqFt helps its customers thrive by offering the information and tools they need to work more efficiently and profitably.

Earlier, Dan was founding CEO and practitioner of an IT, communications and cybersecurity consulting company. Dan is a published and contributing author of numerous white papers, articles and books, and is a frequent and well-respected speaker about software collaboration and cybersecurity.

Office of the Information and Privacy Commissioner, Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: 416-326-3333
Fax: 416-325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

Absio Corporation
8740 Lucent Boulevard, Suite 101
Highlands Ranch, CO, 80129
Telephone: 720-981-2969
Website: www.absio.com

Privacy by Design: www.privacybydesign.ca

May 2014

Information and Privacy Commissioner, Ontario, Canada

Absio®
Take Control of Your Digital World™