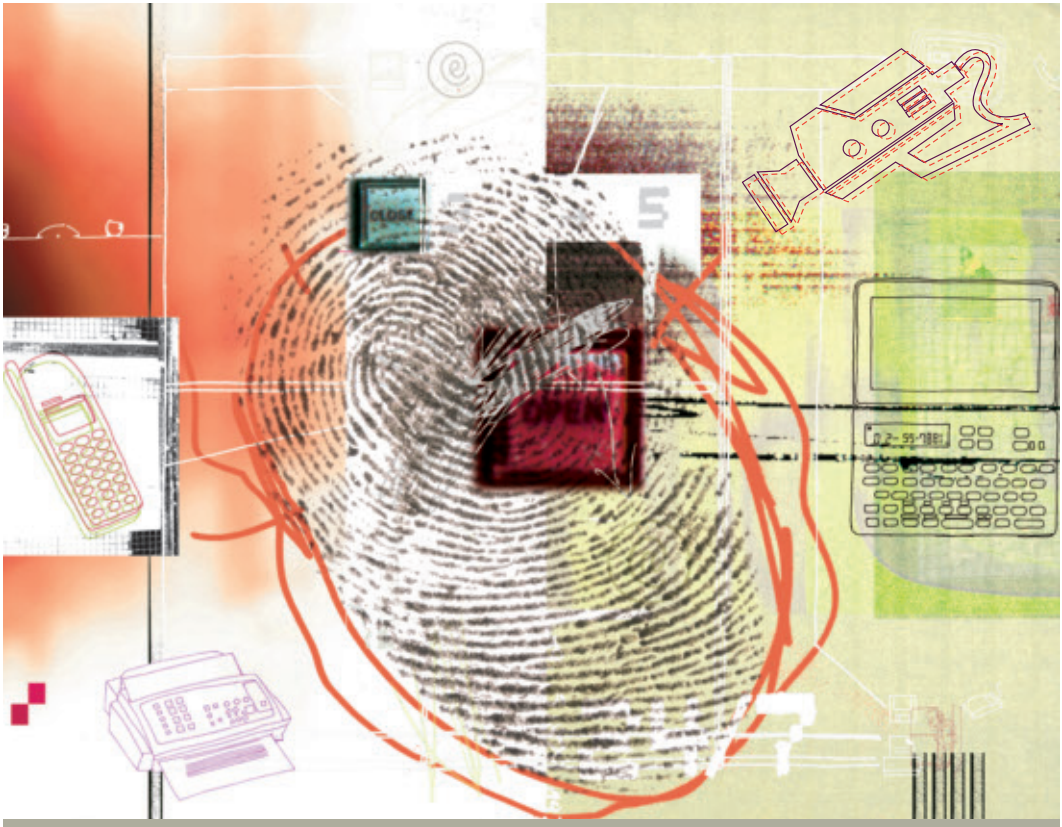

PRIVACY BY DESIGN

...TAKE THE CHALLENGE

Ann Cavoukian, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
CANADA

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

Introduction

For many years, I have argued that privacy is part of the essential foundation upon which free and democratic societies are built. Our right to control the collection, use and disclosure of information about ourselves is the right upon which our other freedoms – freedom of association, freedom of movement, and the freedom to live as we choose – rest. Therefore, to preserve our privacy is to preserve that which we cherish but often take for granted – the freedom and liberty that define the open society in which we live.

It is this understanding that has fuelled my longstanding interest in the privacy rights of individuals, and that has so powerfully cemented my dedication to the cause.

Over the years, I've seen many developments in the world of privacy. I've also seen the world change in ways that no one could have anticipated, even 20 years ago. And with these changes – the growing deployment of biometrics, Radio Frequency Identification, online social networks, and cloud computing, among many others – have come new challenges to privacy and our ability to exercise that right effectively.

But unlike some critics, who see technology as necessarily eroding privacy, I have long taken the view that technology is inherently neutral. As much as it can be used to chip away at privacy, its support can also be enlisted to protect privacy through the use of Privacy-Enhancing Technologies (PETs) – a term that I coined in 1995 with the Netherlands Data Protection Authority. The concept of PETs was predicated on a deeper philosophy – that of embedding privacy into the design specifications of technology itself, thereby ensuring its ongoing presence.

Even in the '90s, it was clear to me that the time was upon us when regulation and policy would no longer be sufficient to safeguard privacy. With the increasing complexity and interconnectedness of information technologies, nothing short of *building* privacy right into system design, in my view, could suffice. So I developed the concept of "Privacy by Design" to capture the notion of embedding privacy into technology itself – making it the default, delivered through various PETs. At that time, this approach was considered to be quite controversial. Now, it is the status quo.

Recently, I've evolved the concept of PETs, extending it to "PETs *Plus*," by adding one new component – a *positive-sum* paradigm. The prevailing zero-sum model, wherein privacy is pitted *against* security, or *against* business practices, is destined to fail – including the failure of privacy. But if you change the paradigm to an *inclusive* positive-sum model, which allows the growth of both privacy *and* security, hand-in-hand, then the future of privacy grows more certain. PETs *Plus* recognizes the role of infrastructure, design, and architecture in enhancing privacy and building user confidence and trust. Take this a step further and you can achieve what I am calling *Transformative Technologies*, which have the power to transform otherwise privacy-invasive technologies into privacy-protective ones – *positive-sum* all the way.

These evolutions have arisen as our rapidly changing world has called into question the prevailing views of how best to protect privacy, now and well into the future. A key characteristic of these evolutions is that they recognize that individual control will play a lesser role in the protection of personal information. With Web 2.0 providing users with fewer and fewer touch-points, controls must become an inherent part of the system.

What has remained constant throughout these evolutions is my firm conviction that a future without Privacy by Design – a future where privacy is not integrated thoughtfully and consistently into the very fabric, the very architecture of technology itself – is a future in which privacy will cease to exist. And with that, many of the fundamental freedoms that we now take for granted, will also begin to erode.

This anthology pulls together some of my Office's most important work in the area of Privacy by Design. It's an area we've been particularly active in over the past two years as some new technologies, like RFID and online social networking, have

exploded onto the scene, raising questions about how they may be deployed in a privacy-protective manner.

In the course of our work, we've been fortunate to form some strong partnerships, working closely with leading organizations such as IBM, Intel, Hewlett-Packard and Facebook to build awareness and encourage the development of responsible approaches to technology. The results of some of these partnerships appear in this anthology.

I fully expect that over the coming years my Office will continue to be active in encouraging the development and uptake of PETs *Plus*. But as our environment becomes more complex, and the threats to privacy increasingly difficult to pinpoint, the path ahead points toward an integrated and expansive model of Privacy by Design.

Whereas our focus has, until now, largely been on building privacy into information technologies, we have now begun to work more closely with organizations, both public and private sector, to also build privacy tools into business practices and into physical design. From data breach protocols to the layout of hospital waiting rooms, opportunities abound to treat privacy as a design concept from the outset, and to achieve privacy objectives alongside other operational goals.

I call this the Privacy by Design Trilogy, and it is my sincere hope that this direction will cement the idea that privacy interests do not operate in a zero-sum model. We need not trade off privacy against other goals like security or transparency. Having more of one does not necessitate having less of the other – quite the opposite. It is indeed possible, desirable, and feasible to have both. And I believe we can do that with the careful application of the principles of Privacy by Design laid out in the pages that follow.

Whatever field you work in or whatever technologies you interact with, I hope that you find the papers collected here to be thought-provoking, and I encourage you to consider ways in which privacy and technology can interact. While this is a small sample of the work that my Office has done, it is perhaps our best. You will find our remaining resources at www.ipc.on.ca. Here's to privacy and freedom – living well into the future.

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

Table of Contents