YOUR RIGHT TO PRIVACY

Minimize Your Digital Footprint

Jim Bronskill and
David McKie

Self-Counsel Press
(a division of)
International Self-Counsel Press Ltd.
USA Canada

Self-Counsel Press acknowledges the financial support of the Government of Canada through the Canada Book Fund (CBF) for our publishing activities.

Printed in Canada.

First edition: 2016

Library and Archives Canada Cataloguing in Publication

Bronskill, Jim, 1964-, author

Your right to privacy : minimize your digital footprint / Jim Bronskill and David McKie.

ISBN 978-1-77040-263-8 (paperback)

1. Privacy, Right of. 2. Computer security. 3. Internet—Security measures. 4. Data protection—Security measures.mI. McKie, David, 1959-, author II. Title.

JC596.B76 2016 323.44’83 C2016-901705-2

Dr. Ann Cavoukian, Executive Director of the Privacy and Big Data Institute at Ryerson University and former Information and Privacy Commissioner of Ontario, provided the Foreword and it is used with permission.

Self-Counsel Press
(a division of)
International Self-Counsel Press Ltd.

Bellingham, WA
USA

North Vancouver, BC
Canada

Contents

Notice to Readers

Laws are constantly changing. Every effort is made to keep this publication as current as possible. However, the authors, the publisher, and the vendor of this book make no representations or warranties regarding the outcome or the use to which the information in this book is put and are not assuming any liability for any claims, losses, or damages arising out of the use of this book. The reader should not rely on the authors or the publisher of this book for any professional advice. Please be sure that you have the most recent edition.

Website links often expire or web pages move; at the time of this book's publication the links were current.

Acknowledgments

The idea for this book emerged from the fertile mind of Self-Counsel Press' former Publisher and Editor-in-Chief, Kirk LaPointe. His idea was for Jim and I to write a companion to our first book, *Your Right to Know: How to Use the Law to Get Government Secrets*. His thinking? The right to privacy is the flip side of the right to information. The rationale was as compelling as it was unassailable. This book just had to be written. So I would like to thank Kirk for convincing two initially reluctant and busy working journalists, teachers, and family men to assume this task.

Also deserving of my gratitude is Dr. Ann Cavoukian, whose words grace the book's foreword. She has been a steady, knowledgeable, and passionate voice for privacy rights dating back to her tenure as Ontario's Privacy Commissioner, and now as the Executive Director of Ryerson University's Big Data Institute.

I would also like to thank all the whip-smart experts who patiently guided us through the research and fielded persistent queries about the intricacies of balancing the reasonable expectation of privacy with the need to surrender personal information in order to enjoy the benefits of life in an increasingly connected world.

I would like to, as I always do, thank my wife, Deirdre; son, Jordan; daughters, Hannah Rose and Leila; and son-in-law Scott, whose love fuels the energy and passion needed to take on these projects. Finally, I want to acknowledge the latest addition to our family, my granddaughter,

Nylah Violet. May she grow up in a world that embraces the ideals that fill the pages in this book — our right to privacy.

— DM

I would also like to commend Kirk LaPointe for his confidence in us and his belief in the need for such a guide. Special thanks go to David for his willingness to explore new terrain with his customary curiosity and enthusiasm. Thanks also to Tanya Lee Howe for her valuable contributions to organizing and presenting our thoughts.

I came to the project with the advantage of much help over the years from so many people who have informed my reporting on privacy and surveillance issues — to them I express sincere appreciation. Anne-Marie Hayden and her indefatigable team at the federal privacy commissioner's office deserve praise for ably fielding my steady stream of questions. I am also greatly indebted to Colin Bennett, Gus Hosein, and Vincent Gogolek for the insights that greatly enliven the pages that follow.

Finally, I thank Lucianne, Adam, and Rose for their patience, support, and understanding, without which this book could not have been written.

— JB

Foreword

The amount of online data is increasing at an alarming rate. Many of our traditional face-to-face interactions — such as banking, shopping, and social connections — are now taking place online. While more knowledge may lead to undeniable economic and social benefits, the availability of data and specialized analytics that are capable of linking seemingly anonymous information can paint an accurate picture of our private lives. This raises significant concerns about the future of privacy. Preserving privacy may depend on our ability to reclaim control of our online information and personal identities, ensuring continued freedom and liberty via privacy and data protection, in the midst of 21st-century technologies.

We are social animals who seek contact with each other, but we also seek privacy: moments of solitude, intimacy, quiet, reserve, and control — personal control. These interests have coexisted for centuries and must continue to do so, for the human condition requires both. To achieve these competing objectives, organizations must embed easily accessible, privacy-protective controls into their services, or what I call, "Privacy by Design." Equally important, though, must be the willingness of each of us to use them. So while much work is required on the part of organizations to gain our trust that they will be upstanding data custodians, as individuals who also independently contribute to our online identities, we too must shoulder some responsibility for our online privacy.

Your Right to Privacy: Minimize Your Digital Footprint makes a valuable contribution to simplifying the complex online ecosystem into

manageable chunks so that each of us is able to understand the implications of our online activities for our privacy. This practical user guide is an encyclopedia of knowledge about privacy and even more, including advice and tips about how we can protect our online identities without needing an advanced degree in science, technology, engineering, or mathematics.

We can, and must, have both — the future of privacy … the future of freedom, may well depend on it. As the saying goes — if you ask for it, it will come. So speak up, get smart, and claim your privacy!

— Dr. Ann Cavoukian,
Executive Director of the Privacy and Big Data
Institute at Ryerson University and former Information and Privacy
Commissioner of Ontario
(ryerson.ca/pbdi/about/people/cavoukian.html)

Introduction

I never said, "I want to be alone." I only said, "I want to be let alone!" There is all the difference.

— Greta Garbo

Digital technology has profoundly changed the way we learn, work, communicate, play, and enjoy culture. It has become such a ubiquitous part of our lives — and brings so many tangible benefits — that we might overlook the not-so-obvious costs.

Perhaps chief among those costs is the surrender of our privacy, threads of personal information from the fabric of our online existence. Sometimes we unknowingly give up the cloak of anonymity through the click of a mouse. But increasingly we are witting participants in handing over personal details as we navigate the online world.

Sharing photos, messages, and our likes and dislikes through social media is fun — not to mention free — and the fact a site such as Facebook harvests our information for commercial purposes in the process just seems part of the bargain. Googling has become a verb, and is now second nature, so we accept the targeted advertising that pops up as a result of our searches.

University of Victoria Political Science Professor Colin Bennett, one of the experts whose opinions we canvassed, put it succinctly: "Our lives are becoming more transparent to multiple organizations."

This book will make you more aware of these transactions, help you better understand them, and show you practical ways to minimize your digital footprint. It is organized around the activities of daily life — at home, at work, in transit, crossing the border and, of course, online.

By the time you read this, there will no doubt be both new ways of interacting with the world that put your privacy at risk and fresh solutions for protecting your personal information. Privacy in the modern age is a fast-moving target, but we hope this guide hits the immediate mark and gives you a sense of where it's all going.

Privacy Principles

The right to privacy has been neatly summarized as the right to be left alone. For our purposes, we will broaden that notion to embrace principles embodied in Canada's federal privacy regime:

- Information should be collected, used, and shared only for specific purposes.
- Data should be stored and disposed of responsibly.
- People should have a right to see information gathered about them.
- Upon being made aware of errors in a personal file, the holder should correct the information.
- People should have the right to complain if personal data is being used for unintended purposes.

In examining an array of issues — from crossing the border to the scourge of identity theft — we will look at how these basic principles apply. Wherever possible, the book will also emphasize what you can do to avoid, address, and remedy potential difficulties each privacy risk might present.

1

Privacy Through the Ages

In the 11th century, defending England from possible invasion by Scandinavia meant having the funds to maintain a robust army. So in 1086, William the Conqueror undertook an ambitious survey of taxpayers across the land.

One observer noted, "There was no single hide nor a yard of land, nor indeed one ox nor one cow nor one pig which was left out."[1] The epic scale of the endeavor would see it compared to the biblical Judgment Day, or Doomsday, resulting in a sheepskin text composed in black and red ink known as the *Domesday Book*.

It seems governments of various stripes have attempted through history to monitor citizens as a means of enriching the treasury or detecting signs of dissent.

The methods of state control exercised by totalitarian regimes are depressingly familiar: Widespread use of informants, pervasive electronic surveillance, a lack of due process, and arbitrary detention.

In his seminal *1984*, George Orwell describes a rigidly controlled society under the ever-watchful eye of Big Brother — one in which omnipresent telescreens monitor citizens and the Thought Police investigate suspected disloyalty. The novel, published in 1949, seemed to anticipate

1 The Domesday Book Online, accessed March 2016. domesdaybook.co.uk/faqs.html

the surveillance states of the Communist Bloc typified by the East German Stasi, which turned neighbor against neighbor in cultivating a vast web of informants.

Though western nations avoided excesses on this scale, the intelligence services of Britain, Canada, and the United States spied on a wide array of citizens who dared question the Cold War political orthodoxy, amassing many thousands of files.

International agreements — including the European Convention on Human Rights and the International Covenant on Civil and Political Rights of the United Nations — began to entrench privacy guarantees. At last count, at least 99 countries have enacted privacy laws.[2]

In Canada, privacy is a quasi-constitutional right enshrined in the *Privacy Act*, governing federal institutions, and the *Personal Information Protection and Electronic Documents Act*, which covers the private sector in concert with similar provincial laws.

A hallmark of the Canadian system is the oversight afforded by the federal privacy commissioner and provincial counterparts, who enforce the laws, serve as ombudsmen for citizens with complaints, and play a watchdog role against invasive practices.

In the United States, the *Privacy Act* governs the collection and use of personal information in the federal government sphere, while the Federal Trade Commission polices the abuse of private data affecting consumers.

Former US spy contractor Edward Snowden's revelations about widespread surveillance of online communication have reverberated in recent years, sparking an international conversation on digital privacy.[3]

In the 21st century, the struggle for privacy is waged not just with governments and law-enforcement agencies but with commercial enterprises that gather, sift, and sell personal data — often without our knowledge but in many cases with our full consent.

The state has a monopoly on a wide range of services and programs that can only be obtained through government, not to mention the ability to restrict or take away our liberty through incarceration, notes Vincent Gogolek, Executive Director of the British Columbia Freedom of Information and Privacy Association.

2 "Global Tables of Data Privacy Laws and Bills," (3rd Ed.), Graham Greenleaf, accessed March 2016. papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875

3 "SNOWDEN: Here's Everything We've Learned in One Year of Unprecedented Top-Secret Leaks," Paul Szoldra, accessed March 2016. businessinsider.com/snowden-leaks-timeline-2014-6

This is not to minimize the role of the private sector, which has access to a growing amount of our personal information, Gogolek adds. “But there is increasing convergence between the public and private sectors in terms of information sharing, and also with the delivery of public services through private-sector partners.”

University of Victoria Political Scientist Colin Bennett goes further. “I don’t think it is possible to tell the difference between the public and private sectors anymore. Governments use the data of the corporate sector for public purposes, and vice versa. In that sense, the Big Brother metaphor is not that useful because the notion of ‘the state’ has radically changed in the last 30 to 40 years. We need theories of surveillance that go beyond Big Brother and which resonate with the real risks and concerns of the general public.”

Against the backdrop of dizzying technological advances, those who wish to minimize their digital footprint find a complex dynamic.