palgrave pivot

TECHNOLOGY OF OPPRESSION

Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance

Elliot D. Cohen

Technology of Oppression

DOI: 10.1057/9781137408211.0001

Other Palgrave Pivot titles

Ilan Alon (editor): **Social Franchising**

Richard Michael O'Meara: **Governing Military Technologies in the 21st Century: Ethics and Operations**

Thomas Birtchnell and William Hoyle: **3D Printing for Development in the Global South: The 3D4D Challenge**

David Fitzgerald and David Ryan: **Obama, US Foreign Policy and the Dilemmas of Intervention**

Lars Elleström: **Media Transformation: The Transfer of Media Characteristics Among Media**

Claudio Povolo: **The Novelist and the Archivist: Fiction and History in Alessandro Manzoni's The Betrothed**

Gerbrand Tholen: **The Changing Nature of the Graduate Labour Market: Media, Policy and Political Discourses in the UK**

Aaron Stoller: **Knowing and Learning as Creative Action: A Reexamination of the Epistemological Foundations of Education**

Carl Packman: **Payday Lending: Global Growth of the High-Cost Credit Market**

Lisa Lau and Om Prakash Dwivedi: **Re-Orientalism and Indian Writing in English**

Chapman Rackaway: **Communicating Politics Online**

G. Douglas Atkins: **T.S. Eliot's Christmas Poems: An Essay in Writing-as-Reading and Other "Impossible Unions"**

Marsha Berry and Mark Schleser: **Mobile Media Making in an Age of Smartphones**

Isabel Harbaugh: **Smallholders and the Non-Farm Transition in Latin America**

Daniel A. Wagner (editor): **Learning and Education in Developing Countries: Research and Policy for the Post-2015 UN Development Goals**

Murat Ustaoğlu and Ahmet İncekara: **Islamic Finance Alternatives for Emerging Economies: Empirical Evidence from Turkey**

Laurent Bibard: **Sexuality and Globalization: An Introduction to a Phenomenology of Sexualities**

Thorsten Botz-Bornstein and Noreen Abdullah-Khan: **The Veil in Kuwait: Gender, Fashion, Identity**

Vasilis Kostakis and Michel Bauwens: **Network Society and Future Scenarios for a Collaborative Economy**

Tom Watson (editor): **Eastern European Perspectives on the Development of Public Relations: Other Voices**

Erik Paul: **Australia as US Client State: The Geopolitics of De-Democratization and Insecurity**

Floyd Weatherspoon: **African-American Males and the U.S. Justice System of Marginalization: A National Tragedy**

Mark Axelrod: **No Symbols Where None Intended: Literary Essays from Laclos to Beckett**

DOI: 10.1057/9781137408211.0001

palgrave pivot

Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance

Elliot D. Cohen

palgrave
macmillan

DOI: 10.1057/9781137408211.0001

TECHNOLOGY OF OPPRESSION

Softcover reprint of the hardcover 1st edition 2014 978-1-137-42621-5

First published in 2014 by
PALGRAVE MACMILLAN®
in the United States—a division of St. Martin's Press LLC,
175 Fifth Avenue, New York, NY 10010.

Where this book is distributed in the UK, Europe and the rest of the world, this is by Palgrave Macmillan, a division of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN: 978–1–137–40821–1 PDF
ISBN: 978-1-349-49075-2

Library of Congress Cataloging-in-Publication Data is available from the Library of Congress.

A catalogue record of the book is available from the British Library.

First edition: 2014

www.palgrave.com/pivot

DOI: 10.1057/9781137408211

Contents

DOI: 10.1057/9781137408211.0001

Preface

The technological turning point has arrived. We now are at a crossroads where we can, potentially, transform human existence into an automated set of commands that monitor and control thought and action for the sake of national security. Or, we can resist the technological thrust or "imperative" toward this dehumanizing end. This latter option is a monumental challenge; for it requires the resolve and cooperation of people throughout the world to press for substantive changes in law, social consciousness, and technology itself.

This book is largely about the logistics of making these changes. It is intended for a diverse population of readers—including the movers and shakers who can help get the job done. It is intended for those who occupy positions of authority in government and the justice system; for those in the industrial sector, who have the means to make available the "meta-technologies" to curb the overreach of primary surveillance technologies; for those in the media who care passionately about their constitutional charge to keep the people informed about the necessity of such changes; and, finally, for the people, themselves, who are subject to government monitoring and control.

For two decades, I have studied information capture and analysis technologies, including their propensity for generating false positives. I have also invented and held U.S. patents in content filtering for electronic message systems.[1] Thus, my interest in mass surveillance technologies is not a passing interest. In 2010, I published the Palgrave Macmillan book titled, *Mass Surveillance and State*

DOI: 10.1057/9781137408211.0002

Control: The Total Information Awareness Project, in which I described a significant amount of what Edward Snowden later confirmed through his leaked documents, although in less detail. This book is a follow-up and update to the previous book in light of these new revelations. The previous book aimed largely at exposing the nature and magnitude of the "Total Information Awareness Project" for purposes of issuing a sobering warning about the steady advance toward a "culture of control." In contrast, the present book tackles, in greater detail, the practical question of how to make constructive changes in order to safeguard the basic values that make human life human.

I wrote this book because I felt the urgency. Now is the time for revamping the manner in which government—that of the United States and its allies—conducts foreign intelligence investigations. This is by sweeping up masses of personal and private electronic information in global proportions, virtually all of which is irrelevant for foreign intelligence gathering purposes. Exposing the true terrorist plot does not require such mass violation of rights. In the aftermath of the Snowden leaks, more people are, at last, asking questions about this program. While the world community is expressing serious concern, it is the best time to get down to particulars about what changes are needed. I hope the specific recommendations for change advanced in this book are useful toward this end.

Note

1 For example, US 5796948, as discussed in the Introduction to this book.

DOI: 10.1057/9781137408211.0002

palgrave pivot

www.palgrave.com/pivot

Introduction: Why Privacy Matters

Abstract: *The Introduction to this book carefully defines the moral and legal significance of privacy, freedom, and dignity. It then discusses the mounting threat posed to these core human values by the technological expansion of mass, warrantless surveillance technologies. Accordingly, it sets the stage for an examination of this technological expansion.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0003.

The rate of development of new tracking and surveillance technologies is progressing at an incredible rate. This progression is moving toward increasingly intrusive devices for gathering information. As this progression continues, unopposed by means to curtail the invasiveness of these technologies, the prospects for the survival of human freedom and dignity in the not-so-distant future are bleak. This is true because these humanizing values are possible only if there remains intact a zone of privacy, which is offline and surveillance-free. Without such a private zone, the most personal decisions become fodder for politico-media-industrial manipulation and control. As more intrusive means of technology advance, and as human beings, with each successive generation, become increasingly accustomed to conducting their personal lives online, this sphere of privacy continues to be eroded. The inevitable result of this forward thrust toward the demise of privacy is the demise of human freedom and dignity, which are dependent on its survival.

Privacy, freedom, and dignity

"Privacy," as understood in the informational context, refers to the state of not having one's personal information shared with others without one's informed consent. Personal information includes the most intimate facts about oneself. It includes information about one's (physical and mental) health, bank records, social security number, and credit history. It includes facts about oneself such as one's age, weight, and one's mental and physical abilities. It also includes personal beliefs, desires, attitudes, and preferences such as one's social and political views, religious convictions (or the lack thereof), sexual orientation, sexual preferences or fantasies; and it includes one's indiscretions, secret rendezvous, lies, legal infractions, and many and sundry other personal things.

There can also be, and often is, a significant difference between one's public persona and one's private self. What one chooses to disclose in public may not truly capture who one truly is. For example, in public, one may be outgoing while privately one may be shy and reserved. Some of us may publicly project an image of caring greatly for others, while, in private, be rather self-centered. Regardless of the moral quality of one's inner, private self, people generally have a right not to share personal information about themselves with others. This right to privacy is both a moral and legal right.

DOI: 10.1057/9781137408211.0003

To say that one has a moral right to privacy means that one has a morally justified claim or interest that others not gain access to one's personal information without one's informed consent; and this right can be said to be violated or abridged when others manage to gain such access. Further, the moral right to privacy derives from a more general right of self-determination, that is, the liberty or freedom to choose for oneself in matters concerning what is one's own, such as one's personal possessions or property, or one's own life—provided, of course, one is a competent adult. Thus, one has such a right to dispose of personal information in any way one sees fit inasmuch as such information is one's own.

This general moral right of self-determination also has legal standing pursuant to the US Constitution. It is enshrined in the Fourteenth Amendment, which holds that no state shall "deprive any person of life, liberty, or property, without due process of law," and the same language is repeated in the Fifth Amendment. The First Amendment holds that "Congress shall make no law…abridging the freedom of speech, or of the press…" But, clearly, without a sphere of privacy in which to speak freely without the government listening, or of the press to gather news without the government eavesdropping on its sources, there can be no protected legal right to free speech, or a free press. Again, the Fourth Amendment recognizes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…" Here is where the Constitution makes clear that the government will, in no case, violate one's personal space without a warrant based on probable cause. In *Olmstead v. U.S.* (1928), Justice Brandeis famously expressed,

> The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality—the right to be left alone—the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect.[1]

The "privacies of life" are, in Justice Brandeis' words, at the core of "man's spiritual nature, his feelings, and his intellect." Foreclose this area of protected freedom or autonomy to be oneself in the privacy of one's

DOI: 10.1057/9781137408211.0003

home, or to dispose of one's personal information as one sees fit, and one's very personhood and individuality—one's unique spiritual nature, feelings, and intellect—is chilled off. The quality of human dignity lies in the respect owed to persons by virtue of their ability to navigate their own ship of life. Dismantle this private sphere of freedom by refusing to leave people alone and an essential condition of their dignity—the ability to freely think and act—is also imperiled.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed.

This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

The power of technology to change who we are should not be underestimated. Few would deny the transformative influences of digital

DOI: 10.1057/9781137408211.0003

technologies on society. Through social media, such as Facebook and Twitter, many of us, especially those of the younger generations, regularly share even the most intimate details of their lives with masses of strangers. To the generation prior to the advent of the internet, a world in which one could speak to millions about a sexual relationship gone awry would have been (virtually) unthinkable. As new forms of digital technologies emerge, such as ones that blur the distinction between the real and virtual worlds; or wherein thoughts themselves, instead of text, can be tweeted; or wherein the "people inside the television set" can really see what you are doing in your living room, we can predictably expect the next generation, now in diapers, to buy into it. Through such successive stages of the technological decline of privacy, the distinction between the private and the public will itself evaporate. In this fishbowl existence, where government knows all (or virtually all), the next obvious step will be to apply this knowledge through more and more technologically sophisticated means of controlling our thoughts and our behavior (for example, downloading executable files into our brains).

How we got here and what to do about it

What drives this forward thrust toward increasing technological change is multifaceted. First, mass surveillance technologies have meant lucrative defense contracts for technology companies, which typically enjoy a revolving door with the US government. Second, the desire for immediate gratification (so-called short-term hedonism) leads us to overlook long-term losses for short-term gratification. Thus, we are more willing to tolerate being monitored as long as it does not affect the quality of our online experience. Third, we tend to downplay the dangers of new technology and play up their positive features. Thus, it is commonly believed that surveillance technologies can protect us by helping to foil terrorist plots, while, at the same time, we tend to play down the dangers of unleashing such technologies without proper privacy protections. Fourth, the so-called "Technological Imperative" speaks to us, "If we can build a new technology, we should build it." This appetite for technological innovation has led us to build weapons of mass destruction, such as biological warfare, even though, rationally, they portend greater evil than good. Indeed, life-altering, even planet-altering technologies have been produced and brought to market in advance of serious reflection

DOI: 10.1057/9781137408211.0003

on the ethical and legal questions they raise. From genetic engineering and nanotechnology to technologies of mass communication, we have moved toward global change on the assumption that the prudential questions about their costs and benefits will somehow be satisfactorily resolved after the fact.

Accordingly, this book attempts to systematically examine and provide rational responses to the ethical and legal quandaries that surround development and deployment of mass, warrantless, and global surveillance technologies. While the treatment here addresses the problem it presents for the American people, it also looks at it from a global perspective; that is, it considers what changes in the present system of surveillance policies and practice the world community would want, and even demand. In this age of Post-Snowden disclosure, much more is publicly available about the National Security Agency's (NSA) mass surveillance program; but this information has been "leaked" in the form of government documents, which have not themselves been systematically examined and connected in order to expose the functional relationships between various parts of a massive, integrated network of technologies. This book provides this systematization and draws out its legal and moral implications.

The President's challenge

In his January 17, 2014 speech on the NSA surveillance program, President Barack Obama indicated his intention to make changes in the program and admitted that there were problems with the system. While he claimed that "some of the worst excesses" that emerged after 9–11 were curbed by the time he took office, he admitted that, "a variety of factors have continued to complicate America's efforts to both defend our nation and uphold our civil liberties." He confirmed that "many routine communications around the world are within our reach"; that, "the government collection and storage of such bulk data also creates a potential for abuse"; that, "the power of new technologies means that there are fewer and fewer technical constraints on what we can do"; and that, "in the absence of institutional requirements for regular debate and oversight that is public as well as private or classified, the danger of government overreach becomes more acute."[2]

DOI: 10.1057/9781137408211.0003

The President has identified crucial issues that can raise substantial challenges to preserving privacy, freedom, and dignity. These problems are succinctly: collection of more data than what is necessary; the potential for abuse; lack of privacy constraints on the technology itself; lack of transparency of surveillance policies and practices. This book takes seriously President Obama's concerns and attempts to address them. In addition, it addresses other related issues including the problem of "backdoor" programs that operate without adequate judicial oversight; exaggeration of the efficiency of various legs of the surveillance network; needless reliance on mass surveillance technologies instead of conventional investigative methods; extending the reach of the program beyond the thwarting of terrorism attacks to "foreign affairs"; interception of privileged communication such as between attorneys and their foreign clients; the dangers of new technologies looming on the horizon.

Some of these problems call for legal changes; some, configuring the technology to better conform to existing law; others, the addition of meta-technologies (technologies to constrain the primary technologies); others, pre-emptive measures to head off the impending dangers of new technologies; and still others, the institution of new policies that promote greater government transparency.

Using content filters to protect privacy

Meta-technologies, which constrain and protect abuses of primary technologies, have been conspicuously lacking in the massive surveillance network that has emerged over several decades. At least documentation has yet to emerge to verify the use of such technologies to protect privacy. Yet, as explained in Chapter 2, such an automatic way to protect privacy is technologically feasible. This book, therefore, emphasizes the use of surveillance meta-technologies and the construction of regulative rules that mandate such use. In particular, it discusses how *content filtering* technologies can be used to guard against needless, unlawful, and unethical acquisition of data by government.

This author has long advocated the use of content filters to preserve privacy, although, historically, there has been a tendency to avoid such use. In 1996, I received one of the first US software patents on a network content filter entitled, *Offensive Message Interceptor for Computers*.[3] According to the background of the invention,

DOI: 10.1057/9781137408211.0003