Information Technology and Law Series

Volume 25

For further volumes:
http://www.springer.com/series/8857

Demetrius Klitou

Privacy-Invading Technologies and Privacy by Design

Safeguarding Privacy, Liberty and Security in the 21st Century

ASSER PRESS

Springer

Demetrius Klitou
Leiden University
Leiden
The Netherlands

ISSN 1570-2782
ISBN 978-94-6265-025-1 ISBN 978-94-6265-026-8 (eBook)
DOI 10.1007/978-94-6265-026-8

Library of Congress Control Number: 2014942017

Published by T.M.C. ASSER PRESS, The Hague, The Netherlands www.asserpress.nl
Produced and distributed for T.M.C. ASSER PRESS by Springer-Verlag Berlin Heidelberg

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Series Information

The *Information Technology & Law Series* was an initiative of IT*e*R, the national programme for Information Technology and Law, which was a research programme set up by the Dutch government and The Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 IT*e*R has published all of its research results in its own book series. In 2002 IT*e*R launched the present internationally orientated and English language *Information Technology & Law Series*. This well-established series deals with the implications of information technology for legal systems and institutions. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Editorial Office

T.M.C. Asser Instituut
P.O. Box 30461
2500 GL The Hague
The Netherlands
Tel.: +31-70-3420300
e-mail: itandlaw@asser.nl

Simone van der Hof, *Editor-in-Chief*
Center for Law in the Information Society (eLaw), Leiden University,
The Netherlands

Bibi van den Berg
Center for Law in the Information Society (eLaw), Leiden University,
The Netherlands

Eleni Kosta
TILT—Tilburg Institute for Law, Technology and Society, Tilburg University,
The Netherlands

Ben Van Rompuy
T.M.C. Asser Instituut, The Netherlands
iMinds-SMIT, Vrije Universiteit Brussel, Belgium

Ulrich Sieber
Max Planck Institute for Foreign and International Criminal Law
Freiburg
Germany

Preface

I find the implications of tomorrow's information society and the advancement of the latest technologies capable of infringing upon the right to privacy and individual liberty extremely relevant, which led me to write this book on the subject.

The discourse in privacy and technology is a legal and political issue, and is more and more a matter of international relations and human rights law. The interplay between politics, ethics, social issues and technology/technological development is a growing phenomenon. Recent examples of the intersection of (international) politics, law, technology and privacy involve the Passenger Name Record (PNR) dispute between the US and EU, the potential worldwide deployment of body scanners, the clash between the European Parliament and EU Council of Ministers over the US-EU SWIFT agreement,[1] and the rift between world leaders and the US Government over recently revealed surveillance activities—just to name a few.

Privacy is a fundamental human right, and deserves just as much attention as any other human right. While there are certainly more grave human rights violations across the globe, particularly in Asia and Africa, here in the West, predominantly in the US and the UK, the threat upon the right to privacy and liberty thereof at the hands of those who control advanced technology is and will remain the story of the early twenty-first century. This is still true, I believe, even in the midst of other highly significant and pressing matters, such as the global fight against terrorism, nuclear proliferation, climate change, environmental disasters and the on-going global economic crisis. Indeed, as technology increasingly advances, in terms of its capabilities in intruding upon privacy, collecting and analysing personal data and conducting mass surveillance, I believe the right to privacy will equally become more and more significant.

It is perhaps during crises, particularly as a result of a major terrorist attack, that governments (and citizens) are more likely inclined to support the further development and deployment of technologies capable of safeguarding security. And, in a

[1] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) manages a global network for exchanging financial messages necessary for facilitating the execution of payment orders/transactions between financial institutions. The US-EU SWIFT agreement allows for the transfer of SWIFT transaction information from the EU to the US.

post-9/11 world, this has indeed occurred. However, the same technologies are often also capable of seriously intruding upon privacy and other civil liberties.

It is important to note that I am certainly not against technology, nor against any governments using technology for maintaining a secure and productive society. I fully support the use of advanced technology, for example, by democratic governments to hunt for terrorists and prevent a terrorist attack, and I recognize that governments are using surveillance technologies to make us safer. They are doing a good job at it. This book does not serve to scaremonger and nor does it argue for the absolute prohibition of surveillance technologies or any other technology capable of invading privacy (i.e., Privacy-Invading Technologies or PITs). I also would like to mostly avoid the social and moral criticism of the rapid development and deployment of PITs. Without arguing against the deployment of PITs, I think we should instead focus primarily on addressing the legal issues at hand and on proposing practical solutions for ensuring that privacy/liberty is always upheld.

The book, instead, serves to point out both the desirable societal benefits and undesirable privacy threats of the latest (privacy-invading) technologies and to recommend how to prevent those threats. I am a technology enthusiast and a supporter of the vast and continuously growing number of digital services (e.g. Google maps, Twitter, etc.) available now online. These are great services. I also especially recognize the infinite possibilities and benefits of technology for society and its well-being. Indeed, for example, the advancement of ICT can address major global societal challenges and provide benefits in terms of commerce, health, mobility, democratic participation, social inclusion, environment and convenience. I am aware that technologies can help governments to serve citizens. Governments use ICT to enhance public security and personal safety and to save lives, for instance, by providing communication capabilities and vital information to first responders, such as digital maps, driving directions, medical information and images. Governments can also use identification technologies, advanced imaging technologies and technologies capable of mass surveillance for better ensuring public/national security. Technology can help us achieve a utopian society.

However, as technology rapidly advances and becomes ever more pervasive, the way and degree to which privacy and liberty may be violated also advances. The right to privacy is becoming ever more difficult to enforce. This has led some to argue that privacy (at least as we know it) will end in the near future, if we do nothing about it (Garfinkel 2001), or is already on its way to ending (Whitaker 2000; Holtzman 2006; O'Hara and Shadbolt 2008), or even has already ended so get over it,[2] and besides what is the use of doing anything about it. At the Centre for Law in the Information Society (eLaw@Leiden), Bart Schermer more specifically argues that privacy will cease to exist in 20 years (2007, 2010). All the same,

[2] For example, Scott McNealy, the former CEO of Sun Microsystems, famously once declared, over a decade ago, "You have zero privacy anyhow, get over it". see Sprenger P. "Sun on Privacy: 'Get over it'", Wired, 26 January, 1999, available at: http://www.wired.com/politics/law/news/1999/01/17538

there is also the strong disbelief that privacy can be concretely ensured in the near future. For some, therefore, the end of privacy and the right thereof is simply inevitable. Accordingly, technology can be used to create a dystopian society.

For these reasons, now more than ever, I believe it is time to thoroughly tackle the great challenges and threats posed by the latest technologies on the right to privacy and other civil liberties, and to thwart the prediction that privacy will end soon. I, for one, also believe that the immense benefits of technology do not have to come at the undesirable expense of privacy and other liberties. A balanced approach is both desirable and possible.

Using all available means and approaches, we must aim to safeguard both privacy/liberty and security in the twenty-first century. If we fail to do so, then we are indeed not just "sleepwalking into a surveillance society" (to quote the UK's former Information Commissioner, Richard Thomas) but, are rather entering into a nightmarish, dystopian, Orwellian future—which has already begun.

Spring 2014 Demetrius Klitou

References

Garfinkel S (2001) Database nation: the death of privacy in the 21st century. O'Reilly Media

Holtzman D (2006) Privacy lost: how technology is endangering your privacy. Jossey-Bass

O'Hara K, Shadbolt N (2008) The spy in the coffee machine: the end of privacy as we know it. Oneworld publications

Schermer B (2010) Privacy and singularity: little ground for optimism? In: Laurens M, Franken H, van den Herik J, van der Klaauw F, Zwenne G-J (eds) Het binnenste buiten; Liber amicorum ter gelegenheid van het emeritaat van Prof. Dr. Schmidt AHJ, Hoogleraar Recht en Informatica te Leiden, eLaw@Leiden, pp 305–319

Schermer BW (2007) Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance. Leiden University Press

Whitaker R (2000) The end of privacy: how total surveillance is becoming a reality. New Press

Contents

Part III New Approach to Protecting Privacy

Part IV Research Results

Acronyms

ABC	Acceptable Behaviour Contract
ACLU	American Civil Liberties Union
ACPO	Association of Chief Police Officers
AI	Artificial Intelligence
ALPR	Automatic License Plate Recognition
AMA	American Medical Association
AMDA	American Medical Directors Association
ASB	Anti-social Behaviour
ASBO	Anti-social Behaviour Orders
ATD	Automatic Threat Detection
ATM	Automatic Teller Machine
ATSA	Aviation and Transportation Security Act 2001
BAT	Best Available Technique
CALEA	Communications Assistance for Law Enforcement Act 1994
CAPPS	Computer Assisted Passenger Prescreening System
CCTV	Closed-Circuit Television
CIA	Central Intelligence Agency
CNN	Cable News Network
COPPA	Children's Online Privacy Protection Act
CPNI	Customer Proprietary Network Information
CTIA	Cellular Telecommunications and Internet Association
CTTL	Clandestine Tagging, Tracking, and Locating
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DNS	Domain Name System
DPA	Data Protection Act 1998
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECPA	Electronic Communications Privacy Act 1986
EDPS	European Data Protection Supervisor
EHR	Electronic Health Records
EPC	Electronic Product Code

EPIC	Electronic Privacy Information Center
ETD	Explosive Trace Detection
EU	European Union
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FEC	Federal Election Commission
FIP	Fair Information Principle
FIPPS	Fair Information Practice Principles
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GAO	Government Accountability Office
GIS	Geographic Information Systems
GLN	Global Location Number
GPRS	General Packet Radio Service
GPS	Global Positioning System
GWOT	Global War on Terror
HIM	Human-Implantable Microchip
HIPAA	Health Insurance Portability and Accountability Act
HRA	Human Rights Act 1998
HSS	HyperSonic Sound
ICCPR	International Covenant of Civil and Political Rights
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
ID	Identification
IED	Improvised Explosive Devices
IID	Improvised Incendiary Device
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITS	Intelligent Transport Systems
ISE	Information Sharing Environment
ISO	International Organization for Standardization
IT	Information Technology
KHz	Kilohertz
LBA	Location-Based Advertising
LBS	Location-Based Service
LEXID®	Lobster-Eye X-ray Imaging Device
LF	Low Frequency
LML	Legal Machine Language
LNL	Legal Natural Language
LRAD	Long-Range Acoustic Devices
LPR	Legal Permanent Resident

LVA	Layered Voice Analysis
MCD	Mobile Computing Device
NGO	Non-governmental Organization
NGR	Next Generation Robot
NIR	National Identity Register
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defense Command
PBD	Privacy by Design
OECD	Organization for Economic Co-operation and Development
PC	Personal Computer
PDA	Personal Digital Assistant
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIT	Privacy-Invading Technology
PLD	Personal Locating Device
PNR	Passenger Name Record
PSCO	Police Support Community Officers
PUF	Physical Unclonable Function
P3P	Privacy Preferences Project
R&D	Research and Development
RFID	Radio Frequency Identification
RIPA	Regulation of Investigatory Powers Act 2000
RTD	Research and Technological Development
SERS	Surface Enhanced Raman Spectroscopy
SOP	Standard Operating Procedure
TATP	Triacetone Triperoxide
TNT	Trinitrotoluen
TRE	Tag Read Events
TSA	Transportation Security Administration
TSO	Transportation Security Officer
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
UDHR	United Nations Declaration of Human Rights
UDI	User-Driven Innovation
UHF	Ultra High Frequency
UHID	Universal Healthcare Identifier
UN	United Nations
US	United States
VIRAT	Video Image Retrieval and Analysis Tool
VCR	Video Cassette Recorder
VSD	Value-Sensitive Design
VSS	Voting System Standards
WBI	Whole Body Imaging
WTMD	Walk-Through Metal Detector