

Comparative Perspectives on Privacy in an Internet Era

CAROLINA ACADEMIC PRESS
GLOBAL PAPERS SERIES

Edited by
Russell L. Weaver and Steven I. Friedland

VOLUME I

Recent Developments in Administrative Law and
Alternative Dispute Resolution

VOLUME II

Comparative Perspectives on Freedom of Expression

VOLUME III

Comparative Perspectives on Administrative Procedure

VOLUME IV

Privacy in a Digital Age

VOLUME V

Comparative Perspectives on Remedies

VOLUME VI

Cybersurveillance in a Post-Snowden World

VOLUME VII

Comparative Perspectives on Privacy in an Internet Era

VOLUME VIII

Free Speech and Media Law in the 21st Century

VOLUME IX

Administrative Law, Administrative Structures,
and Administrative Decisionmaking

Comparative Perspectives on Privacy in an Internet Era

GLOBAL PAPERS SERIES
VOLUME VII

Edited by

Russell L. Weaver

PROFESSOR OF LAW & DISTINGUISHED UNIVERSITY SCHOLAR
UNIVERSITY OF LOUISVILLE, LOUIS D. BRANDEIS SCHOOL OF LAW

Jane Reichel

PROFESSOR OF ADMINISTRATIVE LAW
STOCKHOLM UNIVERSITY FACULTY OF LAW, SWEDEN

Steven I. Friedland

PROFESSOR OF LAW & SENIOR SCHOLAR
ELON UNIVERSITY SCHOOL OF LAW



CAROLINA ACADEMIC PRESS
Durham, North Carolina

Copyright © 2019
Carolina Academic Press, LLC
All Rights Reserved

Library of Congress Cataloging-in-Publication Data

Names: Privacy Discussion Forum (3rd : 2017 : Uppsala, Sweden) | Weaver, Russell L., 1952- editor. | Reichel, Jane, editor. | Friedland, Steven I., editor.
Title: Comparative perspectives on privacy in an Internet era / edited by Russell L. Weaver, Jane Reichel, Steven I. Friedland.
Description: Durham, North Carolina : Carolina Academic Press, LLC, [2018] | Series: The global papers series ; Volume VII
Identifiers: LCCN 2018030818 | ISBN 9781531009571 (alk. paper)
Subjects: LCSH: Privacy, Right of--Comparative studies--Congresses. | Data protection--Law and legislation--Comparative studies--Congresses. | Internet--Law and legislation--Comparative studies--Congresses. | Privacy, Right of--Sweden--Congresses.
Classification: LCC K3264.C65 P753 2017 | DDC 342.08/58--dc23
LC record available at <https://lccn.loc.gov/2018030818>

eISBN 978-1-5310-0958-8

Carolina Academic Press, LLC
700 Kent Street
Durham, North Carolina 27701
Telephone (919) 489-7486
Fax (919) 493-5668
www.cap-press.com

Printed in the United States of America

Contents

Series Note	xi
Introduction	xiii
<i>Russell L. Weaver and Jane Reichel</i>	
Freedom from Fear	3
<i>Luke Milligan</i>	
Introduction	3
I. To Be Secure	6
II. Structure of the Fourth Amendment	9
III. Public Discourse	11
Conclusion	13
Privacy in the Culture of Intrusion	15
<i>Jon L. Mills and Jill Guidera Brown</i>	
Introduction: Human Instincts, Technology, and Culture	15
I. Connection	16
A. Media and Communications	17
B. Connection to Others	19
II. Curiosity	22
A. Pursuit of Knowledge	22
B. Morbid Curiosity	23
C. Innovation	24
III. Convenience	25
A. Predictive Analytics	26
B. Internet-Connected Technologies	27
IV. Security	28
A. Government Surveillance	29
B. Local Law Enforcement	30
C. Public Safety	31
Conclusion: Privacy in the Culture of Intrusion	31

“Is there anybody out there?” — Retention of Communications Data: Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR)	33
<i>Mark D. Cole and Teresa Quintel</i>	
I. Introduction	33
II. Data Protection in Europe — An overview	36
A. The fundamental rights dimension	36
B. The relevant legal texts	39
III. Framework for Communications Data Retention in the EU	41
A. The specific legislative acts	41
B. The CJEU on the Data Retention Directive	44
1) <i>Ireland v EP</i> (2009)	44
2) <i>Digital Rights Ireland</i> (2014)	44
3) <i>Tele2</i> (2016)	45
4) The development in the Court’s approach	46
IV. Relevant Case law by the ECtHR on Mass Surveillance	47
A. <i>Zakharov v Russia</i> (2015)	48
B. <i>Szabó and Vissy v Hungary</i> (2016)	50
C. Consequences for Secret Surveillance Measures	53
D. “Playing Ping-Pong” with the CJEU	54
V. What’s new in the EU? From the CJEU’s <i>Digital Rights Ireland</i> to <i>Tele2</i>	55
A. The application of Article 15(1) e-Privacy Directive as exception clause	56
B. Relationship between Article 1(3) and Article 15(1) e-Privacy Directive	57
C. Requirements for Member States when implementing targeted data retention measures	59
VI. Comparing Standards: Strasbourg and Luxembourg	60
A. The main points found by the ECtHR	61
B. The CJEU’s focus in the <i>Tele2</i> judgment	62
C. Comparison of the Courts’ parallels in the context of data retention and surveillance	64
VII. Retaining other than Communications Data: The case of Financial Data and PNR Data for crime prevention	65
A. The Issue with Financial and Bank Data	66
1. The significance of the Anti-Money Laundering Directive	66
2. Relevant Case law of the ECtHR on Financial Data	69

B. The Issue of Flight Passenger Data Transfer to Third Countries from the EU	72
1. Passenger Name Records Exchange Agreement with Canada	72
2. Mass profiling but not mass surveillance	75
VIII. Looking ahead: Another Brick in the Wall (Part “No-Idea-How-Many-More”)?	78
The Swedish Understanding of Privacy as a Fundamental Right in a Comparative Perspective — Overview and Possibilities	85
<i>Johanna Chamberlain and Jane Reichel</i>	
I. Concepts of Rights and Liberties at the Global Level	85
II. A Slow Start: The Protection of ‘Personal Integrity’ in Swedish Law	87
III. Technological Development, International Impact and the Call for a Swedish Right to Privacy	89
IV. The European Approach to Fundamental Rights, Privacy and Data Protection	91
A. Individual Rights in EU Law — A Tool for Constitutional Effectiveness?	91
B. A European View on Privacy and Data Protection as Fundamental Rights	92
C. Digital Rights Ireland, Google Spain, Schrems, Tele2/Watson and Breyer	95
D. Legislating for Humanity?	98
V. The American Right to Privacy — Civil, Constitutional, Fundamental?	100
A. Going West	100
B. Basic American Provisions	101
C. Establishing a Constitutional Right to Privacy	102
D. Second Thoughts: Does the Constitutional Right to Privacy Exist in the Digital Age?	106
VI. Conclusions	107
A. Looking to the Future	107
B. Closing Thoughts on the American Approach	108
C. Closing Thoughts on the European Approach	109
D. Possible Lines of Development for the Swedish Legal Order	110

Internet Gatekeepers as Editors — The Case of Online Comments	113
<i>András Koltay</i>	
I. Introduction	113
II. Internet gatekeepers as “editors”	116
III. General issues of responsibility for comments	120
A. Comments as “speech”	120
B. Anonymity	120
C. Moderation	122
D. Basis of responsibility for unlawful comments	123
IV. The ECtHR’s case law relating to comments	127
A. Overview of the cases	127
B. Set of criteria shown in the cases before the ECtHR	129
1) The content of the comment	129
2) Identifiability of the commenter	130
3) The content provider’s person	131
4) The person of the affected party	132
5) The effect of the comment on the attacked party	132
6) The conduct of the content provider	133
7) Sanction applied	134
8) Summary	134
V. Main criticism of the ECtHR’s judgments	135
A. Liability of a content provider	135
B. Importance of the “economic service”	136
C. Expecting moderation	137
D. Assessment of the comment’s content	137
VI. Conclusion	139
Privilege, Power, and the Perversion of Privacy Protection	141
<i>Mariette Jones</i>	
I. Privacy protection in the United Kingdom	143
A. Invasion of privacy not a tort in itself	144
B. Reasonable expectation of privacy	146
C. Public interest	147
II. Notion One: Is Privacy protection a tool for the powerful only?	148
A. Privacy injunctions and super injunctions	149
B. Is ‘Data Protection the New Defamation’?	150
C. Data protection in the UK	153
1. Data Protection Act 1998	153
2. EU General Data Protection Regulation	154

III. Notion Two: Modern life entails a de facto surrender of privacy rights	155
A. State sanctioned privacy intrusion	155
B. The European data protection framework	157
C. Deconstructing data protection	158
1. The right to be forgotten — but by whom?	158
2. Informed consent and the (im)practicability of data minimisation	159
3. Echo chambers and confirmation bias: the unintended consequences of content tailoring	161
IV. Concluding remarks	162
A. Some are more equal than others	162
B. Unintended consequences	163
C. Security	163
Accountability in Criminal Discovery	165
<i>Ellen S. Podgor and Louis J. Virelli III</i>	
I. Discovery as a Due Process Obligation	167
A. Blue Book Litigation	167
B. Beyond FOIA	170
II. Discovery and Administrative Law	174
Conclusion	179
Privacy and Free Expression	181
<i>Russell L. Weaver</i>	
I. Free Speech as a “Preferred Right”	183
II. Free Speech and Privacy	186
A. False Light Privacy Claims	186
B. Intrusion Upon Plaintiff’s Seclusion	187
C. Right to Publicity	194
D. Public Disclosure of Private Embarrassing Facts	198
Conclusion	200

Series Note

The Global Papers Series involves publications of papers by nationally and internationally prominent legal scholars on a variety of important legal topics, including administrative law, freedom of expression, defamation and criminal law. The books in this series present the work of scholars from different nations who bring diverse perspectives to the issues under discussion.

Russell L. Weaver*
Jane Reichel**

Introduction

In their landmark 1890 article, *The Right to Privacy*,¹ Samuel Warren and Louis Brandeis sounded the alarm regarding increasing societal encroachments on the right to privacy. Today, with the dawn of the internet era, nineteenth-century technologies and encroachments seem quaint. While the internet has enabled many things, including the ability to communicate more effectively, it has also made it more difficult for individuals to protect their privacy. As Edward Snowden's disclosures revealed, the U.S. National Security Agency (NSA) conducted a massive cybersurveillance that swept up staggering amounts of personal information, including telephone records, emails, text messages, etc. Presumably, other nations are engaged in similar operations. At the same time, businesses mine personal data in order to obtain information regarding their customers' preferences, and more effectively market their products. Moreover, social media companies and internet service providers collect large amounts of information regarding their users' lives.

In 2017, the Privacy Discussion Forum convened at Uppsala University Faculty of Law (Sweden) for the third Privacy Discussion Forum. The event brought together scholars from many different countries to examine privacy issues. Participants were allowed to examine these issues through a variety of lenses, including (but not limited to) Tort, Constitutional Law & Administrative perspectives, as well as from the perspective of media intrusions on individual autonomy, as well as governmental and private uses of information (not only collection issues, but also distribution and use issues). However, a central theme of the discussions was the challenges to privacy created by the internet. The forum produced an interesting array of papers which are published in this book.

* Professor of Law & Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law.

** Professor in Administrative Law, Stockholm University Faculty of Law, Sweden, previously Uppsala University Faculty of Law.

1. 4 HARV. L. REV. (1890).

Professor Luke Milligan's contribution to the forum is entitled *Freedom from Fear*. In that article, he discusses Warren and Brandeis' article, *The Right to Privacy*.² Milligan contends that the Warren and Brandeis view of privacy was multi-dimensional, including both a "breadth" dimension and a "depth" dimension. The "breadth" dimension prohibits government from engaging in physical trespasses, as well as from intruding on individual privacy via other unjustifiable means. The "depth" dimension includes a right to be free of the fear of being subjected to injury. While he notes that the breadth dimension is reflected in the U.S. Supreme Court's interpretation of the Fourth Amendment, as extending to non-physical invasions of privacy, he argues that the depth dimension remains undeveloped. He references the Court's holding in *Clapper v. Amnesty International USA*,³ where the Court held that "the Fourth Amendment is not violated by mere threats or attempts to conduct unreasonable searches or seizures. Nor is it violated by a vast surveillance scheme which just happens to spare the individual claimant." As a result, the plaintiffs in *Clapper* were unable to establish standing to sue because they could not show that the government was actually surveilling them. In other words, under the Court's current interpretation of the Fourth Amendment, there is no protection against the *fear* of unreasonable searches and seizures. There is only protection against actual searches and seizures.

Viewing the matter from an originalist perspective, Milligan argues that the right to be free from fear was very much on the minds of the founding generation. He notes that the Fourth Amendment guarantees "the people" the right to be "secure" in their persons, houses, papers, and effects, and he argues that there are good historical reasons to define the term "secure" as including the right to be free from fear. In making this argument, he resorts to dictionary definitions and historical materials. After mapping out his arguments, he contends that this broader definition of the Fourth Amendment, as including protection of the right to be free from fear, might offer greater protection against U.S. cybersurveillance operations, and might have altered the result in the *Clapper* case. In other word, the plaintiffs in that case might have been able to establish standing to challenge the NSA's cybersurveillance program.

Professor Jon Mills and J.D. Jill Guidera Brown, in their article, *Privacy in the Culture of Intrusion*, suggests that the legal system has not kept pace with advances in technology. While technological advancements have affected and intruded upon virtually every aspect of our lives, they note that "the legal sys-

2. 4 HARV. L. REV. (1890).

3. 568 U.S. 398 (2013).

tem has offered an “unpredictable and sometimes inefficient patchwork of privacy protections.” Indeed, “since many foundational U.S. privacy laws were enacted, society has moved from desktop computers and clunky data processors to sophisticated Internet-connected microcomputers in nearly everyone’s pocket, plus GPS, recreational drones, connected home goods, universal CCTV, Facebook, big data, machine learning, government surveillance, and predictive analytics.” As a result, individuals, motivated by diverse emotions such as “curiosity, cruelty, gossip, jealousy, revenge, anger, and fear” have the ability to penetrate deeply into other people’s lives. However, not only individuals, but also businesses and the government, have used modern technologies to usher “in a global culture of intrusion that only continues to expand as we depend more on mobile devices, peer-to-peer networks, and the sharing economy for daily tasks.” They conclude that, while “the Internet has a history of rugged individualism that preserved free speech at all costs,” that individualism must now be tempered against the “varied privacy and security interests,” and they argue that this “is best done by considering the multitude of cultural and individual triggers that compel us to act in our digital lives.”

Professor Mark D. Cole, and PhD candidate Teresa Quintel, LL.M., submitted a paper entitled “*Is There Anybody Out There?*” *Retention of Communications Data: An Analysis of the Status Quo in Light of the Jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR)*. In their paper, they argue that citizens are subjected to manifold forms of surveillance of their communications. This routine of—often covert measures by national intelligence services, but frequently also by obligation on private parties to retain data of their customers—regular collection and processing of communications data has an impact on the fundamental rights of individuals. Consequently, in a number of cases, European courts have concluded that various surveillance and collection techniques involve unjustified intrusions on privacy or a violation of data protection laws. In their paper, Professor Cole and Ms. Quintel analyze decisions of the CJEU and ECtHR, including the CJEU’s very recent *Tele2/Watson* as well as *Digital Rights Ireland* case, and ECtHR’s judgments in the *Zakharov/Russia* and *Szabó & Vissy/Hungary* cases. The article suggests that the two courts are elegantly working with each other in an effort to protect the privacy rights of European citizens.

Professor Jane Reichel and PhD candidate Joanna Chamberlain in their article, *The Swedish Understanding of Privacy as a Fundamental Right in a Comparative Perspective—Overview and Possibilities*, examine the history and development of the right to privacy in Sweden. In their article, they note that Sweden’s foray into privacy protections began with the creation of the right to

personal integrity. However, it was difficult for Sweden to expand the right of personal integrity for a variety of reasons. For one thing, Swedish jurisprudence, including the school of thought referred to as Scandinavian Legal Realism, suggested that nothing could exist outside of the natural context of time and space, and therefore that immaterial things such as rights could not exist. In addition, freedom of speech and of the press were accorded a higher status than the right of personal integrity, as were the principles of openness and transparency, and therefore privacy rights were subordinated. All of this began to change as new technologies began to infringe on the privacy rights of individuals, and Sweden decided to enact its Data Act. Change was also prompted by Sweden's accession to the European Union, and its decision to become a party to the European Convention on Human Rights, as well as because of the European Union's adoption of its Data Protection Directive. Chamberlain and Reichel use these recent changes to discuss developments regarding the right of privacy in Europe and in the United States, and make suggestions regarding how Sweden can learn from U.S. and European efforts, and bring about change either through constitutional amendment or through case law.

Professor András Koltay's article, *Internet Gatekeepers as Editors—The Case of Online Comments*, examines privacy in the context of the internet, and the posting of online comments. He notes the potential tension between Article 10 and Article 8 of the EctHR, which protect freedom of expression and privacy, respectively, in regard to online comments. He then analyzes European Court of Human Rights decisions regarding the liability of internet participants for such comments. He notes the distinction between "moderated" and "unmoderated" comments, and "active" and "passive" control of websites. Ultimately, he suggests the need for greater clarification and elaboration regarding the rules governing internet service providers. He argues that the need for such rules is apparent given that online comments may be directly related to the public interest, but can also involve hate speech, defamatory material, etc.

Senior Lecturer Mariette Jones's article, *Privilege, Power and the Perversion of Privacy Protection*, examines the tension between individual privacy and the societal need for protection against terrorists, as well as the tradeoffs that societies contemplate in order to protect themselves. She notes that privacy protections run the risk of becoming a tool of the powerful, analogous to the (alleged) abuse of pre-reform libel laws. She also notes that the nature of modern life has led to a *de facto* surrender of privacy rights. Indeed, quoting from the famous Warren and Brandeis article, she argues that a "true understanding of life lived fully in a modern state reveals that the average person is almost *never* 'left alone.'" While she acknowledges that, when privacy interests are weighed against secu-

rity interests, the balance will usually favor security, she questions whether it can “be proven that giving up more privacy rights would necessarily improve the security situation?” Indeed, even though security agencies routinely claim that they were able to thwart terrorist incidents, it is difficult to know whether their claims are true. Everything is conducted in secret. As a result, it is difficult to know whether further intrusions on privacy interests would “have a positive effect on preventing future atrocities when it seems that many of those that do happen seemingly could have been prevented without much intrusion on privacy. For example, questions are raised about the authorities’ failure to take repeated alerts about the Manchester bomber seriously.”

Professors Ellen Podgor and Louis Virelli’s contribution is entitled “*Accountability in Criminal Discovery*.” In their article, they examine recent litigation against the U.S. Department of Justice (DOJ), referred to as the “Blue Book Litigation,” which deals with the tension between the DOJ’s discovery authority in criminal prosecutions and the public’s right to know what its institutions (in that case, DOJ’s exercise of its prosecutorial powers) are doing. The Blue Book, which plaintiffs wished to see, contained information and advice for criminal prosecutors regarding the conduct of discovery in criminal cases. DOJ refused to divulge the contents of the Blue Book on the theory that it involved protected work product and was therefore privileged. Professors Podgor and Virelli take issue with the DOJ’s position, noting that “secrecy outside the confines of a specific case, and more importantly as to policies regarding such procedures, remains questionable” because it directly contradicts the prosecutorial role of being a “minister of justice” and puts prosecutors in the uncomfortable position of seemingly being engaged in what is effectively a “sporting event.” In addition, they argue that the DOJ’s secrecy “flies in the face of key administrative law principles of legitimacy: expertise, accountability, and efficiency.”

Finally, Professor Russell Weaver’s contribution, *Privacy and Free Expression*, examines the tension between the right to free speech and the right to privacy. He notes that, in the U.S., freedom of expression is generally treated as a “preferred right” in the sense that it often prevails over other competing rights. As a result, in competition with the right to be free from defamatory comment, the intentional infliction of mental and emotional distress, or even the right to be free from offensive words, the right to freedom of expression is generally given precedence. The privacy area is a bit unique. While the right to free speech will generally prevail over the right to privacy as well, there are situations when the right to privacy will prevail. Nevertheless, he concludes that there is a significant gulf between the U.S. and Europe with regard to the handling of both free speech and privacy interests. Whereas the U.S. is often very

protective of speech interests, treating freedom of expression as an interest that is entitled to special or preferred protection, European countries are generally more protective of privacy interests. As a result, in many types of privacy cases (e.g., false light privacy and intrusion on seclusion), it can sometimes be difficult for U.S. plaintiffs to prevail against free speech claims. However, in one area, cases involving appropriation of plaintiff's name or likeness for business or commercial purposes, U.S. plaintiffs have been more successful.