The Right to Privacy in the Light of Media Convergence

Media Convergence/ Medienkonvergenz

Edited on behalf of the
Research Unit Media Convergence of
Johannes Gutenberg-University Mainz (JGU) by
Stefan Aufenanger, Dieter Dörr, Stephan Füssel,
Oliver Quiring and Karl Renner

Herausgegeben im Auftrag des
Forschungsschwerpunkts Medienkonvergenz der
Johannes Gutenberg-Universität Mainz (JGU) von
Stefan Aufenanger, Dieter Dörr, Stephan Füssel,
Oliver Quiring und Karl Renner

Volume/Band 3

The Right to Privacy in the Light of Media Convergence

Perspectives from Three Continents

Edited by
Dieter Dörr and Russell L. Weaver

DE GRUYTER

ISBN 978-3-11-027595-7
e-ISBN 978-3-11-027615-2
ISSN 2194-0150

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress

Bibliografische Information der Deutschen Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.dnb.de

Typesetting: jürgen ullrich typosatz, Nördlingen
Printing: Hubert & Co. GmbH & Co. KG, Göttingen
∞ Printed on acid-free paper
Printed in Germany

www.degruyter.com

Table of Contents

About the Authors —— vii

Russell L. Weaver, David F. Partlett and Mark D. Cole
Protecting Privacy in a Digital Age —— 1

Arnold H. Loewy
Is The Right to Privacy Real? —— 31

Craig M. Bradley
Taking Privacy Seriously under the Fourth Amendment —— 37

John A. Humbach
Privacy Rights: The Virtue of Protecting False Reputations —— 51

David Rolph
Politics, Privacy and the Public Interest: A Case Study from Australia —— 65

Jon L. Mills
Privacy and Press Instrusions: New Media, Old Law —— 88

Dieter Dörr and Eva Aernecke
A Never Ending Story: Caroline v. Germany —— 114

Pascal Mbongo
The French Privacy Law
Current questions and forward-looking questions —— **125**

Margareth Etienne
Arrest Records and the Right to Know —— 140

Benjamin W. Cheesbro
Using Open Government to Gain a Competitive Edge
FOIA and Corporate Privacy in the Wake of FCC v. AT&T —— **154**

Sirko Harder
Gain-Based Relief for Invasion of Privacy —— 173

Jan Oster
Breach of Confidence Claims under English and European Private International Law — 194

Andrew Tettenborn
"Confidence-Plus" and Human Rights
The Monstrous New Tort of Breach of Privacy in England — **212**

Normann Witzleb
How should an Australian Statutory Cause of Action Protecting Privacy be framed? — 237

Neil M. Richards
Tort Privacy and Free Speech — 255

Steven Hetcher
Anonymity, Pseudonymity & Online Privacy — 276

W. Jonathan Cardi
Net Negligence
Framework for Understanding Claims for Negligent Infliction of Emotional Distress in the Modern Era — **298**

David Lindsay
Digital Eternity or Digital Oblivion
Some Difficulties in Conceptualising and Implementing the Right to Be Forgotten — **322**

Tobias O. Keber
Secrecy, Privacy, Publicity, Transparency
A German Perspective on WikiLeaks — **344**

Stephanie Schiedermair
Data Protection – is there a bridge across the Atlantic? — 357

Jens-Peter Schneider
European Information Systems and Data Protection as Elements of the European Administrative Union — 374

About the authors

Eva Aernecke: Research Associate at the Chair in Public Law, International and European Law, Media Law, Johannes Gutenberg-University of Mainz, Germany
Craig M. Bradley: Robert A. Lucas Professor, Maurer School of Law, Indiana University, Bloomington, USA
W. Jonathan Cardi: Associate Dean for Research and Development, School of Law, Wake Forest University, Winston-Salem, USA
Benjamin W. Cheesbro: Common Law Lecturer, Johannes Gutenberg-University of Mainz, Germany
Mark D. Cole: Professor of Law, School of Law, University of Luxembourg, Luxembourg
Dieter Dörr: Professor of Law, Chair in Public Law, International and European Law, Media Law, Johannes Gutenberg-University of Mainz, Germany; Director of the Mainz Media Institute
Margareth Etienne: Professor of Law, College of Law, University of Illinois, Urbana-Champaign, USA
Sirko Harder: Senior Lecturer, Monash Law School, Monash University, Melbourne, Australia
Steven Hetcher: Professor of Law, Vanderbilt Law School, Vanderbilt University, Nashville, USA
John A. Humbach: Professor of Law, Pace Law School, Pace University, White Plains, USA
Tobias O. Keber: Academic Council at the Chair in Public Law, European and International Law, Commercial Law, Johannes Gutenberg-University of Mainz, Germany
David Lindsay: Senior Lecturer in Law, Monash Law School, Monash University, Melbourne, Australia
Arnold H. Loewy: George Killam Professor of Criminal Law, School of Law, Texas Tech University, Lubbock, USA
Pascal Mbongo: Professor of Law, School of Law, University of Poitiers, France; President of the French Association of Media and Arts Law
Jon L. Mills: Dean Emeritus, Professor of Law, Director of Center for Governmental Responsibility, Levin College of Law, University of Florida, Gainesville, USA
Jan Oster: DAAD Lecturer in Law, Kings College, London, UK; German advocate (Rechtsanwalt) with FREY Rechtsanwälte, Cologne, Germany
David F. Partlett: Professor of Law, School of Law, Emory University Atlanta, USA
Neil M. Richards: Professor of Law, Washington University School of Law, St. Louis, USA
David Rolph: Associate Professor, Faculty of Law, University of Sydney, Australia
Stephanie Schiedermair: Acadamic Council at the Chair in Public Law, International and European Law, Media Law, Johannes Gutenberg-University of Mainz, Germany
Jens-Peter Schneider: Professor of Public Law and Director of the Department on Public Law, European Information and Infrastructure Law in the Institute of Media and Information Law, University of Freiburg, Germany
Andrew Tettenborn: Professor of Law, School of Law, Swansea University, Wales, UK
Russell L. Weaver: Professor of Law and Distinguished University Scholar, Louis D. Brandeis School of Law, University of Louisville, USA
Normann Witzleb: Senior Lecturer in Law, Monash Law School, Monash University, Melbourne, Australia

Russell L. Weaver, David F. Partlett and Mark D. Cole

Protecting Privacy in a Digital Age

Technological advances have completely revolutionized many aspects of modern society, including the ability to collect, communicate and disseminate information.[1] In ancient times, information, letters and documents moved at the same pace as people, and the pace was inevitably slow.[2] Even Johannes Gutenberg's development of the printing press in the 1500s,[3] which had enormous societal implications by making it possible to relatively quickly create multiple copies of documents, did not enable information to move more quickly (although it did permit the creator of those copies to simultaneously disseminate multiple copies in multiple directions). As a result, although the printing press is widely credited with bringing about the Renaissance, the Scientific Revolution, and the Protestant Reformation,[4] those changes took centuries to occur as information and ideas had to be developed and slowly disseminated.

---

1 See David Crowley & Paul Heyer, Communication in History: Technology, Culture, Society (5th ed. 2007) (hereafter Communication in History); Irving Fang, A History of Mass Communication: Six Information Revolutions (1997) (hereafter A History of Mass Communication); Charles T. Meadow, Making Connections: Communication Through the Ages (2002) (hereafter Communication Through the Ages); Russell L. Weaver, From Gutenberg to the Internet: Free Speech, Advancing Technology and the Implications for Democracy (forthcoming 2012).

2 See James W. Carey, Time, Space and Telegraph, in Communication in History, supra note 1, at 119. The article notes that the telegraph had the effect of diminishing "space as a differentiating criterion in human affairs."

3 See Communication in History, supra note 1, at 82 (noting that some commentators believe that printing "was the major cultural/technological transformation in the history of the West," and that "printing, along with numerous other developments, marked the transition between the end of the Middle Ages and the dawn of the modern era.").

4 See Rogelio Lasso, From the Paper Chase to the Digital Chase: Technology and the Challenge of Teaching 21st Century Law Students, 43 Santa Clara L. Rev. 1, 4 n.2 ("Printing changed every aspect of the human condition–from thinking, learning, and language, to science, religion, and government." "The 17th century became known as 'the century of genius' in large part due to the explosion of creativity and new ideas fueled by printing. Creativity is often the result of a combination of intellectual activities. For example, reading two books on separate topics and combining their themes in one mind produces a creative interaction. Increased output of printed works led first to the combination of old ideas, and later to the creation of entirely new systems of thought."); George Paul & Jason Baron, Information Inflation: Can the Legal System Adapt?, 13 Rich. J. L. & Tech. 1, 8 (2007) ("There has been only one transformative advance in the original writing technology. Circa 1450 Johannes Gutenberg invented the movable type printing press, which dramatically lowered the cost of producing written records. The printing

The speed of information flow began to change dramatically in the nineteenth century as humans gained the ability to control electricity,[5] and learned how to communicate information through electrical impulses.[6] The telegraph, developed in the 1840s,[7] dramatically altered the pace of communication. Prior to the telegraph, the Pony Express could transport a letter from St. Joseph, Missouri, to Sacramento, California, in just 10 days using a relay system of horses and riders.[8] The telegraph could transmit the same message across the entire country in a matter of seconds.[9] Subsequent inventions led to refinements such as radio,[10] television,[11] and satellite, which expanded the impact of electrical impulses by allowing individuals to communicate sound and then images.[12]

Over the last couple of decades, the pace of information flow has accelerated with the development of the Internet.[13] For the first time in history, ordinary individuals can easily access mass communications technologies and can trans-

press allowed mass production of information and thus contributed to the Renaissance, the Scientific Revolution, and the Protestant Reformation.").

5 See Communication in History, supra note 1, at 118 ("With the advent of harnessable electricity, a major shift occurred: The telegraph and telephone became the first wave of a new communications revolution.").

6 See Communication Through the Ages, supra note 1, at 78 (noting that the technology may actually have been invented earlier, but suggesting that the larger amount of credit goes to Samuel F.B. Morse who successfully demonstrated and implemented the technology along with his assistant, Alfred Vail: "Morse's contraption was odd enough to be laughed at. His original receiving equipment consisted of a pen attached to one end of a pivoted arm, with a magnet pulling at a piece of iron attached to the arm. A windup clock motor drew a paper tape under the pen, which marked the tape according to the current flowing through the electromagnet. Morse and Vail continued to improve the device. Eventually, Vail invented a system that used a click key at the transmitted, and a receiver that indented a pattern of dots and dashes on a moving paper tape. Because the instrument made enough noise so the operator could hear the message, the paper tape was abandoned.").

7 See id. at 77–83.

8 Id., at 130–131 ("Before the [intercontinental telegraph] line was completed, the only link between East and West was provided by Pony Express, a mail delivery system involving horse and rider relays. Colorful characters like William "Buffalo Bill" Cody and "Pony Bob" Haslam took about 10 days to carry messages over the 1,800 miles between St. Joseph, Missouri, and Sacramento.").

9 See Tom Standage, Telegraphy – The Victorian Internet, in Communication in History, supra note 1, at 130 (noting that, "as soon as the telegraph along the [Pony Express westward] route was in place, messages could be sent instantly, and the Pony Express was closed down.").

10 See Communication in History, supra note 1, at 204.

11 Communication in History, supra note 1, at 243.

12 See Ruth Schwartz Cohen, The Social Shape of Electronics, in Communication in History, supra note 1, at 313.

13 See From Gutenberg to the Internet, supra note 1.

mit their ideas with ease. Indeed, with the click of a mouse, an individual can post a document on the Web for the entire world to see, and can communicate information around the world through such devices as listserves, websites and blogs.[14] This ease of communication has had profound effects leading to the downfall of long-time leaders in Tunisia and Egypt, and transforming U.S. politics.[15]

The same technologies that have transformed communication have also posed a threat to personal privacy. New computer technologies have made it possible for governments, companies and individuals to collect large amounts of information about each other, and have made it possible to store, analyze and disseminate that information. The implications for personal privacy are staggering. Whereas ancient humans might have been able to maintain a level of anonymity and privacy, modern humans face major challenges as they try to maintain a zone of privacy.

In this short article, we map out the implications of technology for privacy, discuss some of the historical approaches to privacy protection, and offer some suggestions regarding a way forward.

A. Threats from All Fronts

Historically, U.S. citizens have been concerned about protecting their privacy against governmental intrusions. In the modern era, while governmental threats continue to exist, individuals face substantial privacy threats from private sources as well.

I. Government and Surveillance Technologies

Following the American Revolution, the new Americans were primarily focused on privacy concerns that had their roots abuses during the colonial period. Colonist anger had been stirred by the fact that British colonial officials used Writs of Assistance that required them officials to do no more than specify the object of a search in order to obtain a warrant allowing them to search any place

14 See id.

15 See id.

where the goods might be found.[16] The writs were frequently issued without limits on place or duration.[17] The colonists were also aroused by the fact that British officials had used "general warrants" which required only that they specify an offense, but then left them free to decide which persons should be arrested and which places should be searched.[18] Following the Revolution, memories of these British practices prompted the new Americans to demand the protections against "unreasonable searches and seizures" found in the Fourth Amendment to the U.S. Constitution.[19]

---

16 See Virginia v. Moore, 553 U.S. 164, 168–169 (2008) ("The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists."); Samson v. California, 547 U.S. 843, 858 (2006) ("The pre-Revolutionary 'writs of assistance,'" which permitted roving searches for contraband, were reviled precisely because they "placed 'the liberty of every man in the hands of every petty officer.'"); Atwater v. City of Lago Vista, 532 U.S. 318, 339–340 (2001) ("noting that 'the Framers or proponents of the Fourth Amendment' were outspokenly opposed to the infamous general warrants and writs of assistance ...."): see also Russell L. Weaver, Leslie W. Abramson, John M. Burkoff & Catherine Hancock, Principles of Criminal Procedure 64 (3d ed. 2008).

17 See Steagald v. United States, 451 U.S. 204, 221 (1981) ("[The] writs of assistance used in the Colonies noted only the object of the search-any uncustomed goods-and thus left customs officials completely free to search any place where they believed such goods might be."); Gilbert v. California, 388 U.S. 263, 286 (1967) ("The practice had obtained in the colonies of issuing writs of assistance to the revenue officers empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced 'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English and the fundamental principles of law, liberty of every man in the hands of every petty officer.'") (quoting Boyd v. United States, 116 U.S. 616, 625 (19)).

18 See Virginia v. Moore, 553 U.S. 164, 168–169 (2008)("The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists."); Steagald v. United States, 451 U.S. 204, 220 (1981) ("While the common law thus sheds relatively little light on the narrow question before us, the history of the Fourth Amendment strongly suggests that its Framers would not have sanctioned the instant search. The Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and of the writs of assistance used in the Colonies."); Payton v. New York, 445 U.S. 573 (1980)("[The] Fourth Amendment ... grew out of colonial opposition to the infamous general warrants known as writs of assistance, which empowered customs officers to search at will, and to break open receptacles or packages, wherever they suspected uncustomed goods to be"); See Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) ("The general warrant was a recurring point of contention in the Colonies immediately preceding the Revolution. The particular offensiveness it engendered was acutely felt by the merchants and businessmen whose premises and products were inspected for compliance with the several parliamentary revenue measures that most irritated the colonists.").

19 See Maryland v. Garrison, 480 U.S. 79, 91 (1987) ("The Fourth Amendment, in fact, was a direct response to the colonists' objection to searches of homes under general warrants or

The threats to privacy today are strikingly different than the abuses that the colonist's suffered. In the eighteenth century, limited technologies were available for prying into people's lives. Eavesdropping was commonplace, but not always effective. Today, governmental surveillance practices have gone high tech. Governmental officials have listening devices that allow them to overhear conversations from distant locations,[20] even through walls,[21] and they have super-sensitive microphones that allow them to overhear conversations through remotely placed technology.[22] Governmental officials also have the ability to monitor the amount of heat emanating from houses using forward-looking infrared (FLIR),[23] to continuously surveil public places using closed circuit television systems,[24] to detect and ticket speeding motorists with automated technology,[25] to monitor the location of individuals and things using global positioning systems (GPS),[26] and to overhear cell and cordless telephone conversations using special listening

---

without warrants."); See Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) ("[T]he Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance ... [that] granted sweeping power to customs officials and other agents of the King to search at large for smuggled goods.") (quoting United States v. Chadwick, 433 U.S. 1, 7–8 (1977)); Boyd v. United States, 116 U.S. 616, 625 (1886) ("The debate (and the anger) in the American colonies about the arbitrary use of these writs of assistance by the English was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country," and "were fresh in the memories of those who achieved our independence and established our form of government."); see also United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) ("[T]he driving force behind the adoption of the [Fourth] Amendment ... was widespread hastily among the former Colonists to the issuance of writs of assistance .... [T]he purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government.").

20 See Katz v. United States, 389 U.S. 347 (1967) (involving the attachment of an electronic listening device to the outside of a phone booth so that the police could overhear what was being said inside the phone booth).

21 See Goldman v. United States, 316 U.S. 129 (1942) (involving the use of a listening device that allowed the police to overhear what was being said in Goldman's office even though the police were located in an adjoining office).

22 See Silverman v. United States, 365 U.S. 505 (1961) (discussing the fact that advanced surveillance technologies were already available in the 1960s).

23 See Kyllo v. United States, 533 U.S. 27 (2001).

24 See Dina Temple-Raston & Robert Smith, U.S. Eyes U.K.'s Surveillance Cameras, National Public Radio, Weekend Edition Sunday (July 8, 2007). The article can be found at: http://www.npr.org/templates/story/story.php?storyId=11813693.

25 See Ted Robbins, Intense Backlash Against Arizona Speed Cameras, National Public Radio, Morning Edition (Feb. 17, 2010). The article can be found at: http://www.npr.org/templates/story/story.php?storyId=123501023.

26 See City of Ontario v. Quon, 130 S. Ct. 2610 (2010); Devega v. State, 286 Ga. 448, 689 S. E.2d 293 (2010).

devices.[27] Governmental officials also have X-ray technology that allows the police to peer through the walls of homes using drive-by x-ray vans.[28]

As PCs and the Internet have come into common usage, new threats to privacy have emerged. For example, devices have been created that permit individuals to monitor the key strokes and other computer actions taken by someone in a distant location.[29] They and that allow the government to invade the privacy of a person's computer from distant locations through spyware technology.[30]

II. Privacy Threats from Private Individuals and Entities

Even though the focus of the Bill of Rights (essentially, the first ten amendments to the United States Constitution) is on protecting individuals against governmental actions,[31] many modern threats to privacy come from private rather than governmental sources. In the modern era, large corporations collect large quantities of information regarding individuals, and they store, analyze, disseminate and sell that information.

Data collection by private individuals has become a major problem. For one thing, many of the listening devices and other snooping devices that government uses can now be purchased and used by ordinary individuals to spy on the

27 See People v. Ledesma, 206 Ill. 2d 571, 276 Ill. Dec. 900, 795 N.E.2d 253 (2003) (discussing a private individual's interception of a telephone conversation); Kimberly R. Thompson, Cell Phone Snooping: Why Electronic Eavesdropping Goes Unpunished, 35 Am. Crim. L. Rev. 137, 143–44 (1997).

28 See Andy Greenberg, Scanner Vans Allow Drive-By Snooping, Forbes.com (Sept. 9, 2010). The article can be found online at: http://www.forbes.com/forbes/2010/0927/technology-x-rays-homeland-security-aclu-drive-by-snooping.html?feed=rss_technology; see also Rania M. Basha, Kyllo v. United States: The Fourth Amendment Triumphs Over Technology, 41 Brandeis L. J. 939, 939 (2003).

29 See the computer spyware devices sold by the USA Spy Shop at the following URL: http://www.usaspyshop.com/spy-software-c-55.html.

30 See Alan F. Blakley, Daniel B. Garrie & Matthew J. Armstrong, Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware, 2005 Duke L. & Tech. Rev. 25, 1 (2005); Jason Broberg, From Calea to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretap Digital Telecommunications, 77 N. Dakota L. Rev. 795 (2001); Jayni Foley, Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases, 22 Berkeley Tech. L.J. 447 (2007).

31 See, e.g., Lugar v. Edmonson Oil Co., 457 U.S. 922 (1982); Flagg Brothers, Inc. v. Brooks, 436 U.S. 149 (1978); Jackson v. Metropolitan Edison Company, 419 U.S. 345 (1974); Moose Lodge v. Irvis, 407 U.S. 163 (1972).

movement of others,[32] and to monitor what their neighbors or others are saying,[33] even from some distance away.[34] Even pharmacies have been caught "mining" prescription data and selling it to drug companies who use the information to target doctors for sales pitches.[35] The United States Supreme Court continuing the Court's strong free-speech momentum in June 2011 found that the State of Vermont had violated the First Amendment in seeking through legislation to proscribe the data mining practice.[36]

Data and information collection can also be collected in other ways. For example, websites commonly install cookies that allow them to monitor and track those who navigate on to their sites.[37] Indeed, of the 50 most popular U.S. websites, including four Microsoft websites, the sites installed an average of 64 pieces of tracking technology for each person who entered the site.[38] Of course, people voluntarily choose to enter many of these websites, and many are aware of the possibility of cookies. However, individuals may be unaware of the quantity of data being collected about them. Many websites contain privacy policies, often long and sometimes unfathomable by ordinary individuals.

Websites also pose another, and far different, threat to privacy. Inevitably, in a modern technologically-oriented culture, individuals enter personal data onto company websites. In order to make a purchase, they must provide their names, addresses, and credit card information, but this information is not always secure and can be compromised by hackers. For example, recently, hackers penetrated the Play Station Network's security system and access the personal data and credit card information of Play Station customers.[39] It was reported soon after-

---

32 See the GPS systems sold by USA Spy Shop which can be found at the following URL: http://www.usaspyshop.com/gps-tracking-devices-c-118.html.

33 See The Spy Zone, which can be found at the following URL: http://www.spyzone.com/ccp0-display/listeningdevices.html.

34 See the listening device sold at USA Spy Shop at the following URL: http://www.usaspyshop.com/sound-amplifier-system-p-472.html.

35 See Nina Tottenberg, Courts Hears Arguments in Data Mining Case, National Public Radio, All Things Considered (Apr. 26, 2011).

36 Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (6/23/2011) affirmed 2d Circuit in holding the Vermont law unconstitutional as violating First Amendment protections of free speech, http://www.supremecourt.gov/opinions/10pdf/10-779.pdf.

37 See Nick Wingfield, Microsoft Quashed Effort to Boost Online Privacy, The Wall Street Journal, A1, c. 5 (Aug. 2, 2010).

38 See Wingfield, supra note 37, at A1, c. 5.

39 See Eyder Peralta, In Hack, PlayStation Users' Credit Card Data Might Have Been Compromised, National Public Radio, The Two-Way (Apr. 26, 2011). http://www.npr.org/blogs/thetwo-way/2011/04/26/135747338/sony-says-playstation-users-credit-card-data-might-have-been-compromised.

ward that the hackers were attempting to sell the credit card data along with the three number security codes on the back of the cards.[40]

Threats to privacy are also posed by Internet Service Providers (ISP)[41] and search engines.[42] Many ISPs "mine" data from their users' web searches. Indeed, after a federal law required ISPs to make it possible for governmental officials to conduct online surveillance, many ISPs realized that such surveillance could be useful for their own financial purposes:[43] ISPs use this information to determine a user's interests, preferences and tastes,[44] and they sell that information to interested individuals and companies. Unlike websites, which an individual voluntarily enters, and where the individual may at least suspect that information is being gathered, many individuals do not realize that their ISPs are gathering information about them.[45]

Recently, it was discovered that cell phones contain GPS tracking equipment that allows the cell provider to track the user's location. Some phones, such as Apple's iPhone, store information regarding where the phone has been.[46] Google's Android phone collects similar information,[47] as do Microsoft Windows Phones.[48] Indeed, as it turns out, there is no way to disconnect the location-tracking data system.[49] Even if the system is turned off by the user, the phone continues to collect this data.[50] These iPhone location systems are collecting a staggering amount of information. One reporter examined her iPhone and learned that it had recorded an astounding e amount of information about her, including saving some 14,000 text messages, recording some 1,350 words

40 See Eyder Peralta, PlayStation Aftermath: Hackers Claim to Have Credit Card Data, National Public Radio, The Two-Way (Apr. 29, 2011). http://www.npr.org/blogs/thetwo-way/2011/04/29/135844004/playstation-aftermath-hackers-claim-to-have-credit-card-data.

41 See Linda Wertheimer, ISPs Look to Make Money with Mined Data, National Public Radio, Morning Edition (Dec. 27, 2010).

42 See id.

43 See id.

44 See id.

45 See id.

46 See Charles Arthur, iPhone Keeps Record of Everywhere You Go, The Guardian (April 20, 2011). http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears.

47 Id.

48 See Eyder Peralta, As Apple Faces Lawsuit, Microsoft Says Windows Phones Collect Data, Too, National Public Radio, The Two-Way (Apr. 26, 2011).

49 See Eyder Peralta, Reports: There's No Way to Keep iPhone From Collecting Location Data, National Public Radio, The Two-Way (Apr. 25, 2011). http://www.npr.org/blogs/thetwo-way/2011/04/25/135712946/reports-theres-no-way-to-keep-iphone-from-collecting-location-data.

50 Id.

contained in her personal dictionary, 1,450 Facebook contacts, and "tens of thousands of location pings."[51] She was able to use this information "to piece together an hour-by-hour timeline of what she did" on particular days.[52] If such information were freely available, it would not be surprising if analysis of iPhone data became a routine aspect of law enforcement, and is used in civil litigation to obtain additional evidence (*e.g.*, a divorce lawyer might use iPhone data to prove an adulterous relationship).[53] Subsequently, Apple announced that software updates would limit iPhones location information collection to seven days.[54] Two iPhone customers have sued Apple on privacy grounds.[55]

III. Data Storage and Analysis

Of course, beyond the problem of data collection, technology raises serious issues regarding data retention and analysis. Modern technology makes it possible to easily store large quantities of information. Unlike the old days, when companies required large storage areas (sometimes, warehouses) in order to store masses of information, modern electronic systems permit individuals and government to store large quantities of information electronically, and also make it possible to more efficiently search and analyze the stored data.

Technology has also made information more permanent. Since less space is required to store data, not only can more data be stored, but there is less need to

---

51 Id. (Referring to an analysis conducted by Alexis Madrigal of The Altantic).

52 Id.

53 Id. (Again quoting Madrigal) ("Cell phones keep so much information about you," he found, that one forensics specialist said, "mobile device forensics is the future. With the wealth of data even a casual user has stored in his or her cellphone, smartphone, or PDA, it is quickly becoming THE one piece of evidence that is interrogated immediately.").

54 See Eyder Peralta, Apple's Steve Jobs Says Software Update Will Curtail Location Collection, National Public Radio, The Two-Way (Apr. 27, 2011). http://www.npr.org/blogs/thetwo-way/2011/04/27/135779494/apples-steve-jobs-says-it-will-curtail-location-collection.

55 See As Apple Faces Lawsuit, supra note 49. Of great current notoriety has been the hacking of telephones by Mr. Murdoch's "News of the World". The extent of this nefarious practice is startlingly broad and has implicated Scotland Yard. Committee on Culture, Media, and Sport, Transcript of Oral Evidence: Phone Hacking, July 19, 2011, H.C. available online at http://www.parliament.uk/documents/commons-committees/culture-media-sport/Uncorrected_transcript_19_July_phone_hacking.pdf. Scotland Yard is referenced at pp. 69 and 72; Committee on Home Affairs, Unauthorised Tapping Into or Hacking of Mobile Communications, Thirteenth Report of Session 2010–12, H.C., July 20, 2011, available online at http://www.parliament.uk/documents/commons-committees/home-affairs/unauthorised_tapping_or_hacking_mobile_communications_report.pdf.

purge old data and it persist around for long periods.[56] Whereas there was a time when criminal records could be expunged, and effectively disappear from public view, that is rarely the case now.[57] Today, before a record can be expunged, there is a significant possibility that it will be stored in a private data base and continue to live in the database even after expungement.[58] As a result, prospective employers may come across an job applicant's records (even though, in theory, expunged) in doing background checks on applicants.[59]

As data becomes more readily available, websites have been developed which help people access information about others. For example, the website Spokeo.com attempts to estimate people's age, home value, marital status, phone number, home address, hobbies, income, social networks, and it also provides other information.[60] There are other similar websites, including 123people.com, MyLife.com, WhitePages & PeopleFinder.com.[61]

B. The Ineffectiveness of Current Privacy Protections: U.S. Perspectives

The U.S. legal system has not responded effectively to the challenges to personal privacy presented by advancing technology. Both the constitutional protections, and the tort protections, have generally proven inadequate.

I. Constitutional Perspectives

From a constitutional perspective, the principal protection for privacy comes from the Fourth Amendment to the U.S. Constitution which protects individuals against "unreasonable searches and seizures."[62] However, like many provisions

56 See Martin Kaste, Digital Data Make for a Really Permanent Record, National Public Radio, All Things Considered (Oct. 29, 2009). http://www.npr.org/templates/story/story.php?storyId=114276194

57 Id.

58 Id.

59 Id.

60 See Riva Richmond, How to Fix (Or Kill) Web Data About You, The New York Times, B6, c. 1 (April 14, 2011).

61 Id., at c. 2.

62 U.S. Const., Amdt. IV (1791).

of the Bill of Rights, the Fourth Amendment limits only governmental action and not private action.[63] As a result, the Fourth Amendment cannot come close to dealing with modern threats to individual privacy, many of which come from private sources.

Even against governmental intrusions, the Fourth Amendment has provided little protection against the incursions of technology. The Fourth Amendment was written and ratified during the eighteenth century when technology was much more primitive.[64] Indeed, the drafters of the Fourth Amendment were primarily concerned about actual physical searches of their persons, houses, papers and effects.[65] Over the centuries, as technology has exponentially expanded, the United States Supreme Court has struggled to adjust the Fourth Amendment to new technologies. The Court's early definitions of the term "search" and "seizure" tended to track historical understandings by focusing on whether the government had intruded into a "constitutionally protected area."[66] As technology evolved, and it became possible for government to intrude on people without actually entering "constitutionally protected areas,"[67] the Court's interpretations of the Fourth Amendment have not kept pace.

The landmark decision in this area is *Katz v. United States*.[68] In that case, the Court tried to respond to advancing technology by providing that a Fourth Amendment search occurs whenever government intrudes upon an individual's reasonable expectation of privacy.[69] In *Katz*, the incursion came in the form of a listening device attached to the outside of a phone booth, and the Court held

---

63 See, e.g., Lugar v. Edmonson Oil Co., 457 U.S. 922 (1982); Flagg Brothers, Inc. v. Brooks, 436 U.S. 149 (1978); Jackson v. Metropolitan Edison Company, 419 U.S. 345 (1974); Moose Lodge v. Irvis, 407 U.S. 163 (1972).

64 See Russell L. Weaver, The Fourth Amendment, Privacy and Advancing Technology, 80 Miss. L.J. 1131–1227 (2011).

65 See Draper v. United States, 358 U.S. 307 (1959).

66 See, e.g., Goldman v. United States, 316 U.S. 129 (1942); Olmstead v. United States, 277 U.S. 438 (1928); Ex Parte Jackson, 96 U. S. 727 (1877).

67 See id; see also R. Weaver, supra note 64, at 1138–1150.

68 389 U.S. 347 (1967).

69 "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Id., at 351. This "subjective" test was expanded with an "objective" requirement of reasonableness suggested by Justice Harlan's concurrence: "As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation

that the government's use of that device violated Katz's expectation of privacy, noting that "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[70] The Court concluded that:

> what he [Katz] sought to exclude when he entered the booth was not the intruding eye-it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[71]

Although the *Katz* test has provided some protection for individual privacy,[72] the test did not ultimately result in a broad conception of privacy, and the test has not evolved in a way that provided a sufficient response to the challenges of new technology.[73] In its post-*Katz* decisions, the Court has used that test to sustain government's use of various types of technologies to snoop on individuals, including the use of electronic beepers to track the movement of individuals and property,[74] the use of canines (if dogs can be regarded as a form of "technology") to sniff the luggage of passengers,[75] the use of helicopters and airplanes to conduct surveillance and photograph property,[76] and the use of phone records to review an employee's text messages.[77] In *Kyllo v. United States*, 533 U.S. 27 (2001), the Court

---

be one that society is prepared to recognize as 'reasonable.'" Id., at 361 (Harlan, J., concurring).

70 Id., at 351.

71 Id., at 352.

72 See Kyllo v. United States, 533 U.S. 27 (2001) (invalidating the government's use of forward-looking infrared technology that allowed it to determine the level of heat emanating from the roof of a home).

73 See R. Weaver, supra note 64.

74 See United States v. Knotts, 460 U.S. 276 (1983). However, the Court held in United States v. Karo, 468 U.S. 705 (1984), that the use of beepers could be circumscribed to the extent that it allowed government to obtain information regarding the interior of an individual's home.

75 See United States v. Place, 462 U.S. 696 (1983).

76 See Florida v. Riley, 488 U.S. 445 (1989); Dow Chemical Company v. United States, 476 U. S. 227 (1986); California v. Ciraolo, 476 U.S. 207 (1986).

77 See City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

did invalidate the use of forward-looking infrared technology (essentially, a heat detection device) that was pointed at an individual's home. However, *Kyllo* is the exception that proves the rule. As a general rule, the Fourth Amendment has not provided much protection against governmental intrusions on privacy.[78]

Of course, the United States Constitution has been interpreted as including a constitutional right of privacy.[79] However, like many other rights, the constitutional right of privacy protects individuals against governmental rather than private actions.[80] Moreover, that right has generally been interpreted as providing protection only against governmental attempts to limit personal choice on intimate matters such as whether individuals can use contraception[81] and whether a woman can choose to have an abortion.[82] In other words, that right provides little protection against the onslaught of modern technology used by government and individuals to intrude on a person's privacy.

II. Tort Protections

U.S. tort law has also failed to adequately respond to the challenges of technology. Modern privacy theory can be traced to a seminal article written by Samuel Warren and Justice Louis D. Brandeis.[83] In that article, they forcefully articulated the need to protect "privacy," characterizing "the right to be let alone" as "the right most valued by civilized men."[84]

The Warren and Brandeis article led to the creation of the modern tort of invasion of privacy. That tort has four separate and distinct causes of action: 1) intrusion upon the plaintiff's seclusion or solitude, or into private affairs; 2) public disclosure of embarrassing private facts about the plaintiff; 3) publicity that places the plaintiff in a false light in the public eye; and 4) appropriation of the plaintiff's name or likeness for the defendant's advantage.[85]

---

78 See R. Weaver, supra note 64.

79 Griswold v. Connecticut, 381 U.S. 479 (1965); see also Skinner v. Oklahoma, 316 U.S. 535 (1942); Buck v. Bell, 274 U.S. 200 (1927).

80 See id.

81 See Griswold v. Connecticut, 381 U.S. 479 (1965).

82 See Roe v. Wade, 410 U.S. 113 (1973).

83 See Samuel B. Warren & Louis B. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890). For a modern appraisal of the article, its authors and its impact, see Neil M. Richards library article on Warren and Brandeis: The Puzzle of Brandeis, Privacy & Speech, 63 Vand. L. Rev. 1295 (2010).

84 Id.

85 See William L. Prosser, Privacy, 48 Calif. L. Rev. 383 (1960); see also Understanding the First Amendment, supra note 23, at 48–52.

The tort of intrusion into plaintiff's seclusion might lie against someone who uses sophisticated listening or X-ray devices to penetrate the privacy of another person's home. For example, if a paparazzi uses a super-sensitive listening device to overhear conversations within a celebrity's home, or a snoopy neighbor tries to pry into conversations in a neighbor's home, the tort might very well lie.

The difficulty is that the privacy tort has not, to date, been interpreted broadly enough to respond to all of the modern threats to privacy posed by advances in technology. In theory, at least, the tort of public disclosure of private embarrassing facts could be extended to deal with various issues (*e.g.*, ISPs spying on their customers). There may, however, in some instances, be sufficient disclosure to apply the tort. For example, suppose that an ISP mines information from a user's web searches and sells it to a website like Spokeo.com which posts the information on the web. Under such circumstances, the tort might justifiably if one can argue that there has been intrusion on the plaintiff's seclusion or there has been disclosure of private embarrassing facts.

As we note the origins of privacy go back to Warren and Brandeis. Both were conceded about the power of the yellow press in those days to cater to the purient interest much to the detriment of finer society. The technology of the time gave the baser press an ability not possessed by earlier mud rackers how much more may be said today of that capacity. But in the tort arena that privacy interest has retreated in the glaring light of the first amendment as given its triumphal powers by *New York Times v. Sullivan*.[86] For the public official and figure the law of defamation was rendered feckless. The law of privacy, once robust, has been weakened by a series of Supreme Court decisions suggesting that free speech trumps privacy interests. Included are decisions such as *Falwell v. Hustler Magazine*[87] and *Time, Inc. v. Hill*.[88] The free speech bias was affirmed in the Court's recent decision in *Snyder v. Phelps*,[89] a case in which a radical fringe church was allowed to direct the most heinous of assertions at those grieving at the funeral of a dead military servicemen. The case extended speech protections to persons who would attack private persons in the exercise of the most private of social matters in the name of expressions that are a matter of public interest. It follows that the classifications of privacy relating to public disclosure of matters of private interest will be narrowly circumscribed. At the same time false light claims that have always been closely conjoined with defamation will find little favor where the public interest widely writ is involved.

86 376 U.S. 254 (1964).
87 85 U.S. 36 (1988).
88 385 U.S. 374 (1967).
89 131 S.Ct. 1207 (2011).

As a result, protections for privacy must primarily come in statutory form (*e.g.*, anti-wiretapping or anti-hacking laws), and these statutes have proven woefully inadequate to the task.

C. European Perspectives on Privacy

The protection of private data and individual privacy has reached a completely different level in Europe compared to the situation in the United States. There are manifold protections offered to the individual against intrusion into the private life by the State or by third parties, especially where there is a reasonable expectation of privacy such as in their home or even in secluded places in public. In that context, personal data or data about persons are regarded as being an element of the individual that is protected against misuse, as is the person's personality which is protected against the danger of being exposed to complete transparency. Protection of these rights have their source both on a European level as well as in the constitutions of most European States.

On the European, level it is necessary to differentiate between the protection offered by the Council of Europe's legal framework – namely by the relevant Conventions that are signed and ratified by Member States like international treaties – and the European Union, the supranational organization that creates binding law for its twenty-seven Member States and has done so extensively in the field of data protection. In addition, constitutional or statutory protection in some European States go beyond the framework created by these two organizations.

I. The Council of Europe's Framework for Privacy and Data Protection

The Council of Europe has currently forty-seven Member States, each of which (as a condition of membership today) has ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 1950.[90] Although it is an international treaty, and therefore one could assume it only has limited value within national law (as might be the case with the majority of legal

90 The organisation's webpage at www.coe.int, the treaties at http://conventions.coe.int/.

acts under public international law), the reality with the ECHR is somewhat different: not only have many Member States given the Convention a prominent position in their legal order, sometimes even trumping the validity of national constitutional provisions. A key component of the ECHR system is the European Court of Human Rights which has an individual applications procedure that allows any individual to claim that his rights under the Convention have been violated by his specific State.[91] Although the Strasbourg Court may only decide the specific case before it, it effectively interprets the Convention (which it refers to as a "living instrument")[92] in a generally applicable way that provides guidelines for understanding the document in modern contexts. Famous for its standard-setting role concerning the freedom of expression and the media as laid down in Art. 10 ECHR[93] it has played a similar role concerning Art. 8 with its right to respect for private and family life. Although neither a right to personality nor data protection are explicitly mentioned in the provision the Court has interpreted it to encompass both:

> Everyone has the right to respect for his private and family life, his home and his correspondence.
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[94]

Also, the scope of protection has been expanded beyond simply defending individuals against intrusions by the States in that States are also required to protect the private sphere of individuals against intrusions by other individuals.

---

91 The complete case law can be found under http://cmiskp.echr.coe.int/tkp 197/search.asp?skin=hudoc-en.

92 Recently e.g. Case of A, B and C v. Ireland, Application no. 25579/05, judgment of 16 December 2010, para. 234.

93 Cf. e.g. The Sunday Times/United Kingdom (no. 1), Application no. 6538/74, Judgment of 26 April 1979; The Sunday Times/United Kingdom (no. 2), Application no. 13166/87, judgment of 26 November 1991; Observer and Guardian/United Kingdom, application no. 13585/88, judgment of 26 November 1991; Fressoz and Roire/France, application no. 29183/95, judgment of 21 January 1999.

94 On the continuous modernization of the right Nicole A. Moreham, The Right to Respect for Private Life in the European Convention on Human Rights: A Re-examination, European Human Rights Law Review, Issue 1, 2008, p. 44 et seq. Cf. generally on Art. 8 also Udo Fink/Mark D. Cole/Tobias Keber, Europäisches und Internationales Medienrecht, Heidelberg 2008, no. 281 et seq.

This was the basis for the famous rulings in the "paparrazi cases." Limitations of the right need to be justified, i.e. prescribed by law and must be necessary to achieve the legitimate aims in a proportionate manner. Therefore, in several cases the Court had to analyze whether national rules – including judicial decisions – balancing the freedom of expression (including in the media) and the right of a person to be left alone in their everyday life are in conformity with the Convention.

In the famous case of (Caroline) von Hannover v. Germany[95] the Monegasque princess prevailed claiming that German Courts had insufficiently protected her against the publication of photos which inter alia showed her in a private beach club, dining in a remote corner of a restaurant and shopping at a market. Although these activities took place in public or places accessible to a limited part of the public the Court reiterated that Art. 8 protects "a zone of interaction of a person with others, even in a public context."[96] Art. 8 applies if the person has a legitimate or reasonable expectation under the circumstances that what is done or said will remain private.[97] Therefore the passing on of images taken by a CCTV of a person attempting suicide are a violation of Art. 8 even though it happened in a public space, because the person did not need to expect such a dissemination of the event.[98] It is noteworthy that the Court in the Caroline case saw reason for "increased vigilance in protecting private life [...] to contend with new communication technologies which make it possible to store and reproduce personal data"[99]

Recently, the *Caroline* holding has been applied to a UK context in the two cases of *MGN Ltd.* and *Mosley*, both of which emphasize that the principles for protecting prominent persons/celebrities needs to be established by the States themselves rather than by the European Court: "by reason of their direct and continuous contact with the vital forces of their countries, the State authorities are, in principle, in a better position than the international judge to give an opinion on how best to secure the right to respect for private life within the

95 Von Hannover v. Germany, Application no. 59320/00, judgment of 24 June 2004; all ECtHR decisions can be accessed via http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en.

96 Id., para. 50; see also: Peck v. the United Kingdom, Application no. 44647/98, judgment of 28 January 2003, para. 57.

97 Id., para. 51; also Copland v. the United Kingdom, Application no.62617/00, judgment of 3 April 2007, paras. 41 et seq.; generally Gomez-Arostegui, H. Thomas, Defining private life under the European Convention on Human Rights by referring to reasonable expectations, 35 California Western International Law Journal, Spring 2005, p. 153 et seq.

98 Peck v. the United Kingdom, paras. 57, 62 and 85 et seq.

99 Von Hannover, para. 70; cf. also Amann v. Switzerland, Application no. 27798/95, judgment of 16 February 2000, paras. 65 et seq.

domestic legal order."[100] In this context it may be interesting to point out that England, after being reluctant to recognize the tort of privacy, has now adopted the tort in the fashion of the European model where matters of human dignity are given strong protection against free speech concerns. The protection used to flow from the font of confidentiality but recently has become more of a protector of privacy simpliciter. Moreover, the starkest example of privacy protection in England is in the granting of injunctions that prevent not only the revelation of information, but also the identity of those seeking relief. Indeed, injunctions can be granted to prevent publication of the fact of the claim for relief. These are super injunctions that have been much examined recently: A committee was established by the Master of the Rolls in 2010 to review the use of the injunctions.

Recently, Mosley brought an action arguing that he was entitled to a super injunction in respect of the publication of his sexual trysts with prostitutes with an alleged prostitute. Mosley took his case to the European Court of Human Rights. Although helost his case on other grounds (the question was whether the non-existence of a newspaper's obligation to provide prenotification was a violation of Art. 8, and the court, and the court's answer was in the negative, expressing fear such an obligation (if recognized) could violate Art. 10), the Court gave strong indications that Mosley's right to privacy trumps the publisher's right to reveal the story. In *Caroline*, and in *Mosley*, the Court distinguished between "valuable" information contributing to a debate of general public interest in a democratic society and "sensational and, at times, lurid news", i.e. the yellow press celebrity stories, the latter not being able to claim the same robust protection as the first.[101]

In *MGN*,[102] the UK publisher of "The Daily Mirror" was ordered to pay significant legal fees after losing a case regarding publication of photos showing

100 Mosley v. the United Kingdom, Application no. 48009/08, judgment of 10 May 2011, para 108; MGN Ltd. v. the United Kingdom, Application no. 39401/04, judgment of 18 January 2011, para 142. 101 (a) Mosley v. News Group Newspapers Ltd., [2008] EWHC (QB) 1777.

101 Mosley v. the United Kingdom, para. 114, 130 et seq.; MGN Ltd. v. the United Kingdom, Application no. 39401/04, judgment of 18 January 2011, para. 143. Recall that Warren and Brandeis were concerned about the "yellow" press in Boston during the era of the article. The distinction between the refined and the profane is elusive and not favored under U.S. Constitutional law, see Frederick Schauer, Slippery Slopes, 99 Harv. L. Rev. 361 (1985). He later revisits the court's reliance on categorical rules in, Principles, Institutions, and the First Amendment, Supreme Court 1997 Term, 112 Harv. L. Rev. 84, 112 (1998).

102 MGN Ltd. v. the United Kingdom, Application no. 39401/04, judgment of 18 January 2011. On this case cf. e.g. Gavin Phillipson, The 'right' of privacy in England and Strasbourg compared, in: Kenyon/Richardson, New Dimensions in Privacy Law, Cambridge 2006, p. 184 et

model Naomi Campbell leaving a Narcotics Anonymous meeting. Campbell succeeded under the breach of confidence tort which the European Court of Human Rights did not see as a violation of Article 10 of the Convention because the publication of the photos accompanying the story (and giving such further details such as the location of the NA meetings) involved an intrusion into Campbell's private life. However, the fees were regarded as having a chilling effect, and therefore constituted a separate violation of the freedom of expression.[103]

As mentioned, Article 8 is interpreted in a way that also protects personal data against exploitation by the States or others.[104] Although the Court initially was hesitant in using the term "data protection" there is an extensive docket of such cases from the very beginning. Today, the Court has adopted a well-differentiated approach to the different categories of threats to personal data. The Court has not delivered the one case defining the scope of Art. 8 in the context relevant here. It does tend to rely on Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data,[105] which dates from 1981, and has been ratified by nearly all Member States. The Convention contains a very broad definition of relevant data ("any information relating to an identified or identifiable individual" in Art. 2 of the Convention) and its scope provides protection to an individual's fundamental rights in cases of automatic processing of personal data relating to him. Nearly twenty five years after a seminal case concerning the application of Art. 8[106] there is no doubt today that data protection is included in the provision.[107]

Limitations of space prohibit a comprehensive overview of relevant cases, but briefly some examples are mentioned to show how Art. 8 will continue to provide increasing protections for private life in situations that arise in the

---

seq.; an early comparison with the situation after the Caroline-case of the ECtHR in Mark D. Cole, "They did it their way" – Caroline in Karlsruhe und Straßburg, Douglas und Campbell in London – Der Persönlichkeitsrechtsschutz Prominenter in England, Zeitschrift für Rechtspolitik (ZRP) 2005, p. 181 et seq.

103 MGN Ltd. v. the United Kingdom, para 151, on the fees system – although limited to the circumstances of the case – paras. 198 et seq.

104 Extensively on the case law Franziska Böhm, Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards Harmonised Data Protection Principles for EU-Internal Information Exchange, Luxembourg 2011, pp. 55 et seq. (manuscript, in preparation for publication).

105 CETS No. 108, Strasbourg, 28 January 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

106 Leander v. Sweden, Application no. 9248/81, judgment of 26 March 1987.

107 Cf. e.g. Ovey, Clare, White, C.A. Robin, Jacobs/White, The European Convention on Human Rights, 4th ed. Oxford 2006, p. 286 et. seq.

digital age and endanger the (individual's) "management" of his data. These protections have often referred to the positive obligations[108] of State's under Art.8 to ensure protection against intrusions by others, in some cases even involving measures to secure respect within the sphere of relations of individuals between themselves, notwithstanding the margin of appreciation Member States have in how they achieve the goal.[109] The obligation includes safeguards against "modern threats" such as publications on the internet that violate persons right to their personal data[110] or interception, unwanted listening/viewing or monitoring of communication to workplace internet usage.[111] The initial emphasis of the criteria was on data related closely to private life (meaning more "intimate" data) this distinction is becoming less decisive today, as was confirmed in a ruling that concerned the retention of fingerprint data and where the storage of such data was put under strict scrutiny concerning the principle of proportionality and the need for a time limit.[112] In a similar case concerning collection of data by the State the Court explicitly introduced an obligation to erase or rectify personal information[113], which has potential for future application in third-party-cases if indirect horizontal effect is assumed for this constellation, too.

II. The European Union's Approach

Although all 27 Member States of the EU are bound by the above-mentioned framework of the Council of Europe, the level of protection by European Union law must be considered as well. A major development on that front occurred with the entry into force of the Lisbon Treaty on December 1st 2009. That treaty not only changed the face of the European Union (by replacing the old European Community and creating a new EU structure for – in principle – all activities),

108 Concerning Art. 8 cf. Mowbray, Alastair, Cases and Materials on the European Convention on Human Rights, 2nd ed. Oxford 2007, p. 485 et seq. or Heringa, Aalt W., The right to respect for privacy, in: van Djik/van Hoof, Theory and practice of the European Convention on Human Rights, 3rd ed. 2006 Antwerp, p. 739 et seq.

109 Van Kück v. Germany, Application no. 35968/97, judgment of 12 June 2003, para. 70 et seq.

110 K.U. v. Finland, Application no. 2872/02, judgment of 2 December 2008.

111 Copland v. the United Kingdom, Application no.62617/00, judgment of 3 April 2007, para. 42.

112 S. and Marper v. the United Kingdom, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para. 107.

113 Segerstedt-Wiberg and others v. Sweden, Application no. 62332/00, judgment of 6 June 2006, para. 90.

but also and foremost declared binding the so-called Charter of Fundamental Rights of the EU.[114] The Charter had existed since the year 2000 when it was proclaimed by the institutions of the EU without receiving binding legal force. The new Treaty on the European Union, its Art. 6 para. 1, gives the Charter (which is a separate document next to the Treaty on the EU and Treaty on the Functioning of the EU (TFEU)), the same legal value as the Treaties. Whereas so far the Court of Justice of the European Union has indirectly declared the substance of Art. 8 of the European Convention on Human Rights applicable as part of the general principles of Union law, there is now an explicit codification of the principles that supplements the general principles. And it is remarkable that the wording of Art. 8 ECHR exists as a protection of private life in Charter (Art. 7), but that Art. 8 of the Charter creates a specific "Protection of personal data":

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Compliance with these rules shall be subject to control by an independent authority.[115]

The Charter provisions are applicable to the EU institutions and bodies as well as to the Member States when implementing EU law. In that way data protection has to be considered in all activities of the EU, but also by the States e.g. when they transpose or apply a EU directive. Astonishingly, in addition Art. 16 of the TFEU stipulates in the same way a right to protection of personal data as the Charter and requests measures to be prepared by the institutions realizing this protection. This gives data protection a special place in EU law and is in conformity with previous decisions by the Court of Justice. These decisions interpret the key legal act in the area of data protection, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 1995.[116] In the Court's view, the rules of the Directive – a form of legal act that obliges Member States to transpose it into

114 Consolidated Texts to be found under http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML.

115 Charter of Fundamental Rights, Notice No. 2010/C 83/02, published in OJ 2010, No. C 83, p. 389.

116 This is a Directive that sets comparable standards to Convention No. 108 of the Council of Europe.

national law leaving choice of form and methods to the national authorities but binding as to the result to be achieved (Art. 288 TFEU) – are to be interpreted in conformity with Art. 8 of the Convention (and therefore in a modern reading this still applies now also in view of the Charter provision) and exceptions to the protective level concerning data are to be strictly limited.[117]

Concerning the publication of information about other persons on the Internet (and comparable means of distribution e.g. via mobile phones) the Court has held that these can potentially fall under the "journalistic privilege" (and thereby be exempt of the strict rules) if the publication has the sole object to disclose to the public information, opinions or ideas.[118] In a recently decided case the Court applied the new standards (i.e. the Charter) to a situation where recipients of agricultural aid successfully defended themselves against their personal data being published on an official website including a search engine.[119] This website had been installed in order to heighten transparency of the use of public money and the control of it. This was regarded as an important value in EU law, too, but the right to not being exposed to such an extent to the public (including being subject to calculations of their current revenue) lets Art. 8 of the Charter prevail even if the data concerned was related to the profession of the individuals.

The high level of data protection in Europe has been threatened by developments concerning data that passes through electronic communications networks, and is used in electronic communication services. Due to the lack of specific provisions in the general Data Protection Directive 95/46 the EU established sector specific rules applicable to the telecommunications business. Currently, these protections are reflected in Directive 2002/58/EC on privacy and electronic communications as amended by Directive 2009/136/EC.[120] With the

---

117 ECJ, Case C-465/00, Rechnungshof v. Österreichischer Rundfunk and Others, judgment of 20 May 2003, paras. 10, 71 et seq.; Case C-101/01, Lindqvist, judgment of 6 November 2003, paras 42 et seq.; more restrictive as to the scope of application under the former legal order of the Community: joined cases C-317/04 and C-318/04, Parliament v. Council, judgment of 30 May 2006, para. 59.

118 Cf. Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, judgment of 16 December 2008, in which it was not decided for the concrete case but left to the national court that had initiated the preliminary proceedings to evaluate the service in question according to the criteria offered by the ECJ.

119 Joined Cases C-92 and 93/09, Schecke and Eifert/Hessen, judgment of 9 November 2010, paras. 67 et seq. and 80 et seq.

120 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37 as amended by Directive 2009/136/EC of the

introduction of this document in 2002, the EU has now taken a position regarding the storing of "cookies" or the mass sending of spam messages. The recent update – which had to be transposed by Member States until the end of May 2011 – of the Directive is meant to expand its relevance in the communications environment of today by e.g. detailing the rules concerning security of processing of data and thereby attempting to avoid fraudulent access to the stored data of service providers (such as has been recently the case e.g. for the Sony Playstation network, as mentioned above). Further areas covered by the Directive are location data indicating the geographic position of the terminal equipment of a user which in principle can only be processed and stored with consent of the user or subscriber of a service which poses a problem in cases such as the extensive and not in advance announced long-term storing of data of where Apple's iPhones were located at a given time. The revision addresses challenges posed by the increasing amount of spyware attacking personal computers as well as e.g. the spread of RFID technologies. In all cases where a "personal data breach" has occurred providers have extensive obligations on how to react and inform. Finally, enforcement of the high level of data protection rules in that Directive is facilitated.

In addition to the above-mentioned statutes, it is indispensable – especially in a piece exploring the challenges to privacy in a transatlantic perspective – to mention the single probably most controversially discussed normtext in this area: the so-called Data Retention Directive[121] which was passed in 2006 mainly as a reaction to acts of terrorism. With it, the differing rules of the Member States of the EU concerning the obligation of communications service providers, mainly for internet and mobile phone services, to store the data (not the content) relating to the communication event were harmonized. The Directive gives a detailed and extensive list of data that Member States must require providers to store for a period of time between 6 months and 2 years. Although this may seem unsurprising from a U.S. perspective, there were harsh reactions due to this

European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws OJ L 337, 8.12.2009, p.11.

121 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.04.2006, p. 54.

obligation extending to all users, concerning a wide range of information, and for a lengthy period of time which would make potential profiling of users easy. The Court of Justice of the EU has (so far) only decided (in favour of the EU) on the question whether there is a Union competence to pass such a Directive, the fundamental rights issue remains unsolved on that level.[122] Some national Constitutional Courts however have struck down the transposing national laws on the grounds that they violated data protection or privacy rules.[123] The European Commission has only just published an evaluation report and it seems obvious that the Directive will be reviewed with special consideration of the proportionality issue analyzing whether the aim of efficient combating of crimes has not been overemphasized in comparison to the individual's rights so far.[124]

Concerning the use of retained data there is another interesting controversy ongoing in Europe at the moment which has been troubling courts in Member States as well as on the European level alike. In order to protect intellectual property rights the Enforcement Directive[125] requests States to foresee a possibility of Courts to order on request of the rights holder access to information from the internet service provider. These then have to hand out data uncovering the subscriber/user "behind" an IP address. Since the right to demand this information from the provider can be limited to cases where the violation of IP rights took a "commercial scale" and States can also take opposing interests into consideration it remains a hazy picture under what circumstances providers have to ignore the expectation of their subscriber that the data is not given to

122 Upheld in Case C-301/06, Ireland v. Parliament and Council, judgment of 10 February 2009, cf. also Fink/Cole/Keber, supra note 94, no. 298 et seq.

123 Bundesverfassungsgericht, 1 BvR 256/08, judgment of 2 March 2010 (Federal Constitutional Court of Germany); Czech Constitutional Court, Official Gazette of 1 April 2011, judgment of the Constitutional Court of 22 March on the provisions of section 97 paragraph 3 and 4 of Act No. 127/2005 Coll. on electronic communications and amending certain related acts as amended, and Decree No 485/2005 Coll. on the data retention and transmission to competent authorities (Press Release, Constitutional Court of the Czech Republic, Ústavní Soud Zrušil Část Zákona o Elektronických Komunikacích [Constitutional Court Struck Down Part of the Electronic Communications Act] [in Czech, with link to the decision] (Mar. 31, 2011)); an unofficial English translation of the Czech case can be found at http://www.edri.org/files/DataRetention_Judgment_ConstitutionalCourt_CzechRepublic.pdf; Romanian Constitutional Court, Decision no. 1258 from 8 October 2009, Romanian Official Monitor No. 789, 23 November 2009.

124 Evaluation report on the Data Retention Directive from the Commission, COM(2011) 225 final, 18.4.2011, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf, cf. esp. p. 32.

125 Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 195, 2.06.2004, p. 16.

third parties. As the Court of Justice of the EU confirmed that the balancing of the opposing fundamental rights of property and data protection has to be performed by the Member States without a specific outcome because both rights also exist in EU law[126], there is no alternative to finding solutions on national level and these may well be diverging.

Concluding the European perspective, it is noteworthy that the enforcement of privacy both in the sense of being left alone from publicity and as data protection is based fully on a fundamental rights understanding that is very robust. It relies less on damages or other forms of remedies though this as well as statutory sanctions such as fines for misdemeanour may apply in addition. Also, both the Council of Europe framework with the ECHR and the specific Data Protection Convention as well as the multifaceted protection just as threats in and by the EU which then affects the Member States are not static but are currently undergoing developments in a judicial and political dimension.

D. Conclusions & the Way Forward

When Warren and Brandeis first called for recognition of the "right to be left alone," they could hardly have envisioned the threats to privacy created by advances in technology. Over the last century, technology has continued to advance and now poses a substantial threat to individual privacy. New forms of technology have allowed both governments and private interests to collect, store, analyze and disseminate information about others. Unlike earlier times, when people could live in relative anonymity, few people find it easy to preserve anonymity today.

Existing constitutional provisions, statutes and case law have not proven adequate to deal with existing threats to individual privacy. In the United States, constitutional provisions have provided insufficient protection against modern threats to privacy. For one thing, most constitutional rights apply only against the government, and private interests pose a major threat to privacy today. In addition, the Fourth Amendment to the United States Constitution, which provide the most significant protections against governmental intrusions, has been restrictively construed so that it provides an insufficient shield against govern-

126 ECJ, Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, judgment of 29 January 2008. Cf. on this also Fink/Cole/Keber, supra note 94, no. 131.

mental attempts to use technology to snoop into people's lives. Tort law provides one avenue of redress, but has hardly proven adequate to address the significant challenges to personal privacy posed by advances in technology. Despite extensive scholarship on privacy as a protectable right, U.S. political economy finds few instances of where the right is protected at the cost to other rights and interests.

In most respects, Europe is farther along than the United States in its efforts to protect privacy. This does not only concern areas where freedom of speech is affected by limitations due to the right to privacy – such as in the "celebrity cases" – because of a less extensive understanding of free speech in this respect, but also the data protection field. This can be clearly seen in the fact that after entry into force of the Data Protection Directive it was regarded to develop a safe harbour principle under which organizations can agree to comply to certain standards laid down in a Commission decision and accompanying documents and thereby making transfer of personal data from Europe to this third country possible in the first place.[127] However, also in Europe new forms of threats have been identified and the revision of the EU's key Data Protection Directive of 1995 is shortly before going underway.[128] In that context the Commission has announced that the guiding principle for revision will remain that every individual is owner of his data and therefore has right to take them back from others that have been processing them. This right will have to go hand-in-hand with an obligation of these parties (such as the Internet Service Providers) to provide solutions for efficiently deleting the personal data (key words are the "right to be forgotten" or "right to withdraw" along with a "digital eraser").[129]

In order to effectively address modern privacy issues, international cooperation and international standards are necessary. Electronic communication methods are no longer confined to a single country. Given that information now readily crosses international borders, and can be mined, store, analyzed and communicated from foreign countries, an individual nation's attempt to deal with privacy issues on its own is doomed to failure even though national

127 Cf. Commission Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7 et seq. as well as http://www.export.gov/safeharbor/.

128 Cf. background information under http://ec.europa.eu/justice/policies/privacy/review/index_en.htm.

129 Id., cf. also Commissioner Viviane Reding in her opening speech at the 6th European Jurists' Forum, 19 May 2011, Luxembourg or in the speech http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/305.

constitutional requirements might oblige the upholding of (isolated) national rules to safeguard a high level of data protection irrespective of what happens elsewhere.

It is doubtful that the gap between privacy protection in Europe and the United States will ever be completely bridged. The idea of "human dignity" that has so ensconced itself in Europe since the Second World War finds scant attention in the U.S. discourse which is dominated by free-speech rhetoric flowing from the First Amendment.

Highlighting the remarkable gap between European and Commonwealth, on the one hand, and US jurisprudence, on the other is that the very idea of prior restraint of publications, let alone an injunction of the strength of a super injunction is anathema to First Amendment principles. Free speech will trump privacy as is the story since *New York Times* and confirmed vividly in the Supreme Court's decision in the military funeral case.[130] However, free speech principles will not preclude all privacy protections in the United States. Most free speech precedent is focused on public officials, public figures, or matters of public interest. Indeed, in the *Phelps* case, the focus was on the public dialogue. When privacy intrusions focus on private individuals, in contexts where issues of public debate are not presented, governmental control might be permissible.[131]

It is to be observed however that the super injunction (as used by the U.K. courts) is weak given the realities of the modern Internet. Even in those cases where the injunctions has been awarded, public curiosity the market place and the irrepressible force of the internet often leads to the revelations of names. And although we suggest the pursuit of treaties it is doubtful that the United States would sign onto the granting and enforcement of super injunctions. So long as servers in California, for example, publish the material the injunction will be a futile exercise in those cases where the public has a thirst for details. Unfortunately this tends to be that base arena of celebrities involved in base activities. It seem that little has changed in the public's taste since Brandeis wrote in the late 19th century. This may show that privacy is a protean matter and that an international approach ought to find common values after dialogue and work piecemeal on those areas. A small seed was sown in the recent G8 summit where in addition to government representa-

130 Cf. Snyder v. Phelps, 131 S.Ct. 1207 (2011).

131 The Supreme Court in Bartnicki v. Vopper, 532 U.S. 514 (2001), leaves room for the tort implying that if the material lacks "newsworthiness" the legitimate degree of protection of privacy is enhanced.

tions and submissions, powerful private actors, Google and Microsoft, participated.[132]

In order to provide effective protections for privacy, an international approach is required. The Internet has provided a major boost to free speech and communication by allowing individuals to directly communicate with each other. Through the wonders of modern technology, individuals can quickly and easily disseminate information around the world. By posting information on websites or blogs, individuals can make such information accessible to individuals in distant lands. However, the same technology that allows information to quickly and easily cross borders also allows for privacy threats to cross borders. As a result, if a single nation develops strict privacy laws, those laws may be evaded by off-shore mining and data disclosure systems.

For that reason it seems attractive and most promising in view of a meaningful defence of privacy standards to think about developing global or at least wide-spread international standards and enforcement mechanisms. This could happen in form of setting by an international treaty a minimal level of protection for all ratifying States which then impose it in their national laws. In a similar way this approach was chosen (for a very limited context) with the Cybercrime Convention of the Council of Europe[133] which was developed with external non-member States and opened for ratification which the U.S. have done meanwhile.[134] In terms of negotiating the approach chosen participating States should certainly not follow the work on the Anti-Counterfeiting Trade Agreement (ACTA) which only after massive protests was made more transparent and – as a result – ended with much less far-reaching proposals as originally planned.[135]

If a new Privacy Treaty is developed, it should include (at least) certain basic concepts. First, privacy protections must be mandatory, and must be backed up by the possibility of both civil and criminal sanctions. A number of ISPs and web browsers have discussed the possibility of developing voluntary programs designed to help ensure individual privacy. The reality is that ISPs and web browsers have a fundamental conflict of interest that prevents them from effec-

---

132 President Nicolas Sarkozy, Press Conference at the G8 Summit, May 26, 2011, http://www.g20-g8.com/g8-g20/g8/english/for-the-press/news-releases/press-conference-by-the-president-of-the-french.1325.html

133 Convention on Cybercrime of 23. November 2001, CETS No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

134 For a list of signatures and ratifications http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

135 Cf. the European Commission's information website http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/.

tively engaging in self-regulation. Even if a company has a desire to help individuals protect their privacy, the company has a conflicting economic interest in betraying that privacy for cold hard cash. All too often, the economic interest is likely to trump the privacy interest.

Second, the treaty should provide strong protections to people in their homes. Even if technology exists which allow individuals to peer into other people's houses, or overhear conversations taking place in those houses, governments can agree to make such snooping devices illegal. If a human being is entitled to privacy anywhere, the protection should extend to conversations and activities that take place privately within a home.

Third, the treaty should include some sort of "Internet Bill of Rights." Even though ISPs, websites and companies may have the ability to mine data from those who use those services, there is nothing preventing the government from making the mining or disclosure of such data illegal.

Fourth, in regard to cell phones, and devices like the iPhone, Android or Windows Phone, the treaty should it make clear that location tracking data and other storage data should be optional with the phone's user. If the user of the phone wishes to disconnect any particular type or storage or location system, that should be the user's option.

Of course, negotiation of an international treaty will not be easy or simple. Nations may differ significantly in terms of what they regard as fundamental values, and those values may make it difficult to find common ground on some privacy issues. For example, in the case of von Hannover v. Germany, discussed earlier, the European Court of Human Rights held that even in public places there can be a reasonable expectancy of being "in private". It is doubtful that such a privacy approach would survive First Amendment scrutiny in the United States. Because Caroline was in public, it is difficult to argue (under U.S. law) that the media cannot take her picture. Thus, while there are possible avenues for U.S. cooperation in terms of a treaty governing the Internet, U.S. negotiators will need to tread lightly in order to ensure that they do not transgress the boundaries established by the First Amendment to the United States Constitution. In addition, American notions of the impropriety of prior restraint would not allow injunctive relief as in the case of superinjunctions to get to first base or to use a cricketing term get off a duck. From a European perspective on the other hand strict data protection standards will be essential, because e.g. the location data issue that would play a role as mentioned above is already regulated in a way that it cannot be used without the subscriber's consent and that these have to be given a possibility to reject the storage. Therefore, presumably the only workable forum would be the Council of Europe because of the high standards already applicable via the Conventions which would remain intact aside a new

treaty. If it were a different organization (e.g. for communications issues one could in principle think of UN organizations like the International Telecommunications Union (ITU) that so far was mainly limited to technical aspects of networks) the European States would have to insist that the other participating States would follow the standards from the Council or at least not undermine them, otherwise the cooperation would not be possible.

A severe challenge and one likely to hamper U.S./European concord on a treaty is the permissible scope of individual contracting out from protection. It is difficult for users to decide to give permission when the future is uncertain, indeed unknowable and an individual's preferences are bounded by rationality and human foibles. Using a simple example: it used to be a straight-forward decision on whether you wanted to be included in automatic listings of telephone numbers in telephone directories or not or whether you wanted the recipient of a phone-call to see your telephone number in the display or not, and it was not difficult to judge on the potential dangers of this. It is a completely different story to decide whether you want to use a smart phone with all its extra functionalities beyond voice communication and are prepared to pay the price of accepting a significant number of transfer of data; judging potential threats here is much more complex and since most users want to use the extra functionalities (and in some context such as social networks often seem hesitant to take care of their privacy) it is sometimes difficult to argue that there needs to be a protection beyond the contractual agreements between the parties. However, as the extent of the processing of data is often not known or the effects impossible to evaluate for the end user States under their obligation to protect might have to limit the possibility of giving up all rights contractually or at least empower the individual to "check out" of the system with the consequence of his stored data having to be (efficiently) deleted and removed from the databases it was entered into.

Arnold H. Loewy

Is The Right to Privacy Real?

Privacy is a term bandied about a lot. Indeed, it is the raison d'etre for this conference. In this paper, I seek to examine how serious concepts of privacy really are in informing decisions that march under its name. Being an American academic, I will focus on the two greatest uses of the term: (1) the constitutional right to privacy, illustrated by such cases as Roe v. Wade[1] and Lawrence v. Texas,[2] and (2) the Fourth Amendment, which the court sometimes speaks in terms of "reasonable expectation of privacy."[3]

A. The Right to Privacy

All sorts of questions have been considered under the right to privacy. Among others, the right to privacy encompasses contraceptives, the right to abortion, the right to assisted suicide, and the right to engage in homosexual activity. What is common about a lot of these activities is that they involve more than one person, and some of them aren't even performed in the home.

Let us begin with abortion, one of the first targets of those who hate an expansive right to privacy.[4] But abortion is not usually performed in the privacy of one's home. Rather, it is performed in a hospital or other medical facility and involves a patient and her doctor. None of this suggests that Roe and its progeny were wrongly decided, only that privacy has nothing to do with the case. To illustrate, compare a law requiring certain anesthesia to be used during a tonsillectomy or another altogether forbidding lap band operation. While these laws might make some people unhappy, I do not believe that these notions of unhappiness would be predicated on the concept of privacy.

The twin rationales for protecting the right to abortion are procreation and personal autonomy. While of course the act done to start the procreation process is normally done in private (at least one would hope), the act to prevent

1 Roe v. Wade, 410 U.S. 113, 116 (1973).

2 Lawrence v. Texas, 539 U.S. 558, 562 (2003).

3 See, e.g., Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

4 See Robert A. Burt, Alex Bickel's Law School and Ours, 104 Yale L.J. 1853, 1859 (1995) (stating that opponents of the extension of the Griswold v. Connecticut "right to privacy" principle in Roe argue that the Constitution does not explicitly protect a right to privacy).

unwanted procreation is not. Candidly, I am not convinced that abortion really is about procreation. If it were, one would think that the question of whether to bring a pregnancy to fruition, or to terminate it, would be one jointly made by the potential mother and father. Yet, the Supreme Court could not be clearer in holding that when the mother and father differ; the mother prevails regardless of the relative equities in a particular case.[5] Indeed, the Court has gone so far as to invalidate a statute requiring notification to the father prior to abortion.[6] So, given that the right to terminate a pregnancy resides exclusively in the mother, traditional notions of equal protection sex discrimination[7] suggest that procreation is not really the reason.

Rather, abortion is really about personal autonomy. The claim is not really about the right to destroy a fetus; it is about the right to not be compelled to carry a fetus as an unwanted appendage to the claimant's body. Obviously, the answer to the personal autonomy claim depends in part on whether one views the fetus as a benign uterine tumor, a human being, or something in-between.

I suppose that privacy could be defined narrowly or broadly. In its broadest form, I would suppose that anything that interferes with a personal "private" choice interferes with privacy. So, at one level, a law that interferes with A's private choice to murder B interferes with privacy. As far as I know, nobody seriously defines privacy that broadly. And, I might add, even if A embellished his argument with "I can now rest more peacefully in the privacy of my home, knowing that B is gone," we would not seriously regard this as an argument from privacy.

To some extent, the case for abortion is the same as far as privacy is concerned. To be sure, there is the very plausible argument that fetuses are worth less than postnatal humans; consequently, their intentional destruction should be permitted.[8] But this argument does not sound in privacy.

The one argument that does sound a bit in privacy is the argument that the fetus is with me wherever I am. His presence makes it more difficult to sit, stand, work, play tennis, have sex, and etc. But again, this equates privacy with personal autonomy. It is indeed quite analogous to the woman who is displeased because lap band procedures have been banned in her jurisdiction. Both women want to remove what they perceive as unwanted invasions of their bodies (a

5 See Planned Parenthood v. Danforth, 428 U.S. 52, 69 (1976).

6 See Planned Parenthood v. Casey, 505 U.S. 833, 895–99 (1992).

7 See Craig v. Boren, 429 U.S. 190, 208–09 (1976) (holding that sex-discriminatory statute was invalid).

8 At least by or at the direction of the fetus's mother.