

Cambridge Intellectual Property and Information Law

Internet Privacy Rights

Rights to Protect Autonomy

Paul Bernal



CAMBRIDGE

INTERNET PRIVACY RIGHTS

Rights to Protect Autonomy

PAUL BERNAL



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org

Information on this title: www.cambridge.org/9781107042735

© Paul Bernal 2014

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2014

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

Bernal, Paul, 1964–

Internet privacy rights : rights to protect autonomy / Paul Bernal.

p. cm. – (Cambridge intellectual property and information law ; 24)

Includes bibliographical references and index.

ISBN 978-1-107-04273-5 (hardback)

1. Data protection–Law and legislation. 2. Computer security–Law and legislation.

3. Internet–Security measures. 4. Internet–Safety measures. 5. Privacy,

Right of. I. Title.

K3264.C65B49 2014

323.44'8–dc23

2013045717

ISBN 978-1-107-04273-5 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

INTERNET PRIVACY RIGHTS

Internet Privacy Rights analyses the current threats to our online autonomy and privacy, and proposes a new model for the gathering, retention and use of personal data. Key to the model is the development of specific privacy rights: a right to roam the internet with privacy, a right to monitor the monitors, a right to delete personal data, and a right to create, assert and protect an online identity. These rights could help in the formulation of more effective and appropriate legislation, and shape more privacy-friendly business models. The conclusion examines how the internet might look with these rights in place and whether such an internet could be sustainable from both a governmental and a business perspective.

PAUL BERNAL is a lecturer in information technology, intellectual property and media law at the University of East Anglia Law School, where his research centres around privacy and human rights, particularly on the internet.

CAMBRIDGE INTELLECTUAL PROPERTY
AND INFORMATION LAW

As its economic potential has rapidly expanded, intellectual property has become a subject of front-rank legal importance. *Cambridge Intellectual Property and Information Law* is a series of monograph studies of major current issues in intellectual property. Each volume contains a mix of international, European, comparative and national law, making this a highly significant series for practitioners, judges and academic researchers in many countries.

Series editors

Lionel Bently

Herchel Smith Professor of Intellectual Property Law, University of Cambridge

William R. Cornish

Emeritus Herchel Smith Professor of Intellectual Property Law,
University of Cambridge

Advisory editors

François Dessemontet, Professor of Law, University of Lausanne

Paul Goldstein, Professor of Law, Stanford University

The Rt Hon. Sir Robin Jacob, Hugh Laddie Professor of Intellectual Property,
University College, London

A list of books in the series can be found at the end of this volume.

PREFACE AND ACKNOWLEDGEMENTS

Privacy on the internet has never mattered more. The internet is now part of almost every aspect of our lives, from the personal and intimate to the professional, from our finances to our leisure, from our interactions with each other to our interactions with our governments. It is no longer something optional, something that we can avoid: if we want to live full lives, to participate in society, to take advantage of all our opportunities, we need the internet.

What happens to us on the internet impacts upon our autonomy – our freedom to act, our freedom to decide for ourselves how we live our lives – and not just our autonomy online but our autonomy in the ‘real’, offline world. Part of this impact arises from the way that our privacy is infringed upon, directly and indirectly, intentionally and unintentionally, by a wide variety of people, companies and government agencies. People are increasingly becoming aware of these problems: internet privacy issues, once of interest to only those loosely described as geeks and nerds, are now headline news all around the world. Internet privacy not only matters, but it is beginning to be seen to matter.

It has been argued that privacy is ‘dead’, that privacy is ‘outdated’ and even that privacy is in itself damaging and that we should embrace transparency and openness in its place. These arguments are not trivial or simplistic, and there is evidence to support all of them, but ultimately they are fundamentally flawed. If we want autonomy, if we want freedom, we need privacy to protect it. We need privacy *rights*.

This book presents a linked set of internet privacy rights – rights that, sometimes even without knowing it, people are already starting to claim. These are not ‘legal’ rights in a precise and enforceable sense, but something more akin to natural rights. They reflect the rights that people *believe* that they have, that people *need* to have in order to function freely on the internet. What these rights are, why they are appropriate and how they could help people and help shape the internet into a more privacy-friendly form in the future is the main purpose of *Internet Privacy Rights*.

Some people express concern primarily against invasions of privacy by the likes of Google and Facebook, some by government agencies such as the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) – particularly in the light of the PRISM, Tempora and related revelations of 2013 – while others seem worried most by criminal scammers and identity thieves. Which of these groups is right? In different ways, each of them has very legitimate concerns, but they cannot be considered separately. The relationships between businesses and governments are complex and intertwined, and criminals and scammers can feed off both. Data gathered by businesses can be accessed and used by government agencies, or hacked or stolen by criminals. Business models based on privacy invasions can be legitimised by governments against the interests of individuals as a result of lobbying, or from the tacit understanding that both businesses and governments can benefit from having more and more information about us.

This is where the rights presented here come in: they can help people to fight their corner. Rights provide a language for people to use, a way to express themselves in the face of what often seems to be the overwhelming power of both the corporate and the security lobbies.

Internet Privacy Rights starts with a theoretical analysis of both privacy and autonomy, and how they apply in the current, substantially commercial form of the internet. It sets out a model – the *Symbiotic Web* – to explain the current, principally commercial way that the internet functions, with individuals dependent on free or discounted services and businesses relying on their ability to gather and use our personal data. This symbiosis is currently essentially beneficial to both individuals and businesses, but there are significant risks attached. Those risks are both analysed theoretically and illustrated through case studies of situations familiar to most people from their everyday experience on the internet. Some of the most common activities on the internet are examined: the use of search engines, the way that behavioural advertising works and so on. The rights suggested in *Internet Privacy Rights* emerge from these case studies: in part as a solution to the problems encountered and in part as a reflection of the way that people, in practice, have responded to those problems.

A number of concepts are introduced in this book: the aforementioned model, the *Symbiotic Web*; *Collaborative Consent*, a new way to look at how to deal with the thorny issue of consent in the online context; *Autonomy by Design*, taking privacy by design a stage further; *Disclosure Minimisation*, a privacy-friendly way of looking at the assertion and

verification of identity; and *Surveillance Minimisation*, addressing the rising issue of government surveillance of the internet. Each of these concepts addresses potentially critical issues that arise from an examination of how the internet currently functions: *Internet Privacy Rights* looks at the internet from both a conceptual and a pragmatic perspective.

This book is a development of the work that I undertook for my PhD thesis at the London School of Economics, and some of the ideas in this book have previously been published (Bernal, 2010a, 2010b, 2011a, 2011b). I should like to thank the LSE and the Arts and Humanities Research Council who provided the funding for the research, and in particular my two excellent PhD supervisors Professor Conor Gearty and Professor Andrew Murray. The central premise of this book joins their two fields – human rights and internet law – and without their expertise, encouragement and support this book would never have been written. I should also like to thank Professor Alastair Mullis whose support at the UEA was invaluable, and my other excellent colleagues at the UEA Law School. Most of all, I would like to thank my daughter Alice for keeping me grounded and reminding me what really matters, and my wife Corina for emotional support, vital assistance with editing and proofreading, and much, much more.

The internet world – particularly insofar as it concerns privacy – is in a state of flux. At the time of writing, that world was still reeling from Edward Snowden's whistle-blowing over PRISM, surveillance and censorship laws and rules were being implemented or contemplated all over the world, and Europe was in the throes of an almost tortuous reform process over data protection. Predicting the future is, as a consequence, fraught with danger. I am not what Morozov might describe as a cyber-utopian, but neither am I a full-fledged 'cyberdystopian', seeing the internet either now or in the future primarily as a tool for authoritarianism and control. The research into internet privacy that is the background to this book reveals a great many problems, some of which seem almost to be insurmountable, but it also reveals some progress, both in practice, with 'victories' for those supporting privacy, and also a significant improvement in awareness of privacy issues. The internet is not, by any stretch of the imagination, 'privacy-friendly' at present – but that does not mean that it is impossible for it to become, at least in some ways, more privacy-friendly.

I believe an improvement might be possible. Whether it will happen is another question entirely. It is very hard to tell, and there are signs in both positive and negative directions. In some ways I suspect a more

privacy-friendly internet is inevitable – the more we know, the more we seem to care, and ultimately companies and governments have to take account of that. At the moment, however, that seems to be a very long way away, but it is of great importance for anyone interested in autonomy and freedom, and not just on the internet.

CONTENTS

<i>Preface and acknowledgements</i>	<i>page ix</i>
1 Internet privacy rights	1
1 Introduction	1
2 Privacy and autonomy on the internet	12
3 Internet privacy rights	15
4 The impact of internet privacy rights	19
5 A privacy-friendly future?	22
2 Privacy, autonomy and the internet	24
1 Autonomy	24
2 Privacy	32
3 Autonomy and consent	36
4 Autonomy, privacy, challenges and criticisms	42
5 Privacy is not the enemy	50
3 The Symbiotic Web	53
1 The Symbiotic Web	53
2 The make-up of the benign symbiosis	60
3 The risks of a malign symbiosis	65
4 Governments and the Symbiotic Web	73
5 Managing the symbiosis	77
4 Law, privacy and the internet – the landscape	82
1 The role of law in the internet	82

2	Privacy-protective law	87	
3	Privacy-invasive law	97	
4	Privacy-related law: the overall landscape	111	
5	Navigating the internet	117	
1	Search engines and their role	117	
2	Google and the Article 29 Working Party	122	
3	Implications and ways forward	131	
4	Conclusions and rights-based solutions	139	
6	Behavioural tracking	144	
1	Behavioural tracking and targeting	144	
2	Does any of this matter? Isn't it just about advertising?	147	
3	Phorm	151	
4	The rise and fall of Phorm	160	
5	Regulation of behavioural tracking	166	
6	Ways forward and rights-based solutions	172	
7	Data vulnerability and the right to delete	176	
1	Vulnerability and autonomy	176	
2	The reality of data vulnerability	181	
3	Data vulnerability – solutions?	197	
4	A change in assumptions and the right to delete	200	
8	A rights-based approach	207	
1	Putting the rights together	207	
2	Autonomy by design	215	
3	A rights-based approach?	223	
4	Rights and symbiotic regulation	230	

9 Privacy and identity	234
1 Online identity	234
2 The privacy, identity, anonymity model	237
3 The concept and creation of identity	240
4 The assertion of identity	247
5 The protection of online identity	250
6 Identity in a privacy-friendly internet	259
10 A privacy-friendly future?	263
1 A need for internet privacy rights?	263
2 An internet with rights	269
3 The internet of the future and addressing critiques	278
4 A transparent society or a privacy-friendly future?	283
<i>Bibliography</i>	291
<i>Index</i>	300

Internet privacy rights

1 Introduction

Privacy on the internet has gone from being a subject of interest only to what might loosely be described as ‘geeks’ and ‘nerds’ to something that is of relevance to almost everyone. The internet is huge business. Facebook has more than a billion users worldwide.¹ Apple, whose products are almost all internet based – the ‘i’ in ‘iMac’, which led to the ‘i’ in iPod, iPhone and iPad, originally stood for ‘internet’² – and Google are two of the world’s three biggest corporations.³ For all of these organisations, privacy has become increasingly important. Data breaches have started to become front-page news. Privacy policies and practices are now taken far more seriously; whenever Mark Zuckerberg announces a new product or service for Facebook, he makes privacy one of the key things that he talks about.⁴ The authorities, too, are taking privacy more seriously: in the United States, for example, Google and Facebook have been made subject to Federal Trade Commission (FTC) privacy audits for twenty years, and Twitter for ten.⁵

Why has privacy become such a big issue? Do we need a new approach to understanding it? These are questions that have been coming more and more to the fore. Amongst other things, this book attempts to explain

¹ Facebook passed 1 billion active users in October 2012: see their press release at <http://newsroom.fb.com/News/457/One-Billion-People-on-Facebook>.

² When Steve Jobs first introduced the iMac in 1998, he said ‘iMac comes from the marriage of the excitement of the Internet with the simplicity of Macintosh’.

³ See for example <http://online.wsj.com/article/SB10001424127887323539804578264024260588396.html>. In January 2013, in terms of market capitalisation Apple was the second largest and Google the third largest corporation in the world.

⁴ When launching Graph Search in January 2013, Zuckerberg said ‘We’ve built Graph Search from the start with privacy in mind, and it respects the privacy and audience of each piece of content on Facebook.’ See <http://newsroom.fb.com/News/562/Introducing-Graph-Search-Beta>.

⁵ For Facebook see www.ftc.gov/opa/2011/11/privacysettlement.shtm, for Google see www.ftc.gov/opa/2011/10/buzz.shtm, for Twitter see www.ftc.gov/opa/2011/03/twitter.shtm.

why and to suggest a way forward. The key to that approach is an understanding that the key reason that privacy has become important is that privacy matters to people, at least in part, because people care about their autonomy, and privacy is a crucial protector of autonomy.

When people care about something, ultimately that finds its way into how businesses react, and how governments react. That is why both businesses and governments are beginning to take privacy seriously. As the case studies in this book reveal, however, that process is taking a long time, and there has been a lot of pain and misunderstanding along the way. The ideas presented in this book are intended to help to reduce that time, and to minimise the pain and misunderstanding. The starting point to that is to have a better understanding of the role that the internet plays in people's lives. From there we can start to understand what people expect from the internet, and what they believe their *rights* should be while they operate on the internet.

1.1 *The internet in contemporary life*

For most people in what might loosely be described as the developed world the internet can no longer be considered an optional extra, but an intrinsic part of life in a modern, developed society. Significant aspects of life take place on the internet. Interactions with government, for example, are becoming increasingly electronic, not only in terms of access to information but more directly and interactively: the completion of tax returns, access to health services,⁶ interaction with local government, and much more. Indeed, the UK government is moving to a 'digital by default' policy.⁷ The digital economy has already become a significant part of the economy as a whole, and this is increasing all the time. In the UK, it is predicted that by 2016, 23 per cent of all purchases in this country will be made online.⁸ It is increasingly the case that people who are not able to access products and services online are at a significant disadvantage, being unable to take advantages of discounts for insurance,⁹ better interest rates

⁶ See www.nhsdirect.nhs.uk/. NHS Direct is suggested as the first port of call for health problems in the UK.

⁷ See <http://digital.cabinetoffice.gov.uk/about/> – Digital by Default is central to the UK government digital strategy.

⁸ See www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/.

⁹ Aviva insurance, for example, in February 2012, was offering a 20 per cent discount for online applications for car insurance. See www.aviva.co.uk/car-insurance/.

on savings,¹⁰ and having tighter deadlines for the submission of information, for example.¹¹ Moreover, there are some very useful services that are only available online, such as price comparison sites for insurance and other financial services.¹² Shopping has been revolutionised, from specialised online services such as Amazon and auction sites such as eBay to the online versions of existing supermarkets, allowing ordering online and delivery to your home.¹³

All this is without considering the most direct, ‘traditional’ uses of the internet, as an unparalleled source of information, for educational or recreational purposes, as an increasingly important news source,¹⁴ or simply to discover practical information such as the location and opening hours of shops, events and so forth.

Perhaps even more important is not the extent to which a capacity to use the internet is now required but the reality of how much it is used in practice. The numerous sites and services noted above are only a small part of what has become a significant element of life. There are many others that have become part of the social fabric for a large section of society. Social networking sites are just one example. They cannot generally be said to be either practically necessary or economically advantageous but they are used, extensively and increasingly, and not just by young people. The same can be said of a whole range of other services, from message boards and blogs to media services such as YouTube.

Further, the internet is no longer something that is only to be accessed through computers. More and more devices can and do use or provide a connection to the internet, from smartphones and tablet devices to Blu-ray players, TV receivers, game machines and digital cameras. This trend appears certain to increase, and increase rapidly,

¹⁰ Most UK banks offer ‘e-savings’ accounts or equivalents, only accessible online, offering better interest rates or other advantages.

¹¹ UK tax returns submitted on paper, for example, are required to be submitted by 31 October each year, while online submissions are allowed until 31 January the following year. See www.hmrc.gov.uk/sa/deadlines-penalties.htm.

¹² E.g. www.gocompare.com/, www.confused.com/, www.comparethemarket.com/.

¹³ See www.amazon.com or www.amazon.co.uk, www.ebay.com and, for example, www.sainsburys.co.uk/home or www.tesco.com/ for online stores of supermarkets.

¹⁴ In the 2008 US election, for example, the Internet was one of the most important sources of news for voters, particularly for young people. Pew Internet Research reported that ‘42% of those ages 18 to 29 say they regularly learn about the campaign from the internet, the highest percentage for any news source’. See <http://people-press.org/report/384/internets-broader-role-in-campaign-2008>.

as the advantages of using internet connections for all kinds of devices become more apparent, and more innovative ideas such as Google's Glass¹⁵ are developed.

The ultimate implication of this is that living without using the internet places people at a significant disadvantage in many different ways, including socially, culturally, democratically and financially. The concept of a 'digital divide', or more accurately 'digital divides',¹⁶ between those who have the skills and opportunities to take advantage of digital services and those who don't, has been discussed since the 1990s – see for example the work of Norris (2001) and Mossberger (Mossberger *et al.*, 2003). The nature of the relevant divides has changed considerably over the last decade, as the role that the internet plays in society has become more significant, as outlined above, and access to it has become the norm rather than the exception. The disadvantages to those who do not have internet access are continuing to grow both in scale and breadth, which is one of the reasons why there are increasing calls to consider access to the internet a 'right'.

The idea of internet access as a basic human right has been put forward by many, and according to a large survey by the BBC World Service, nearly 80 per cent of people around the world believe that it should be.¹⁷ In Estonia,¹⁸ France¹⁹ and Greece,²⁰ for example, internet access has already been made a constitutional right, while in Finland this right has become

¹⁵ Google Glass is a headset designed to be worn like glasses, 'reading' what you see and providing a 'heads-up display' of relevant data before your eyes. See www.google.com/glass/start/.

¹⁶ Divides between rich and poor nations, between the rich and the poor within nations, between the better and worse educated, between the urban and the rural, divides based on gender, disability, race and more – there are many possible reasons for what might be termed digital disadvantage. Mossberger also identifies different aspects of the divides – what she terms the 'access divide', the 'skills divide', the 'economic opportunity divide' and the 'democratic divide', paralleling some of the discussion in this chapter. See Mossberger, Tolbert and Stansbury (2003, particularly p. 9).

¹⁷ http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf. The survey included more than 27,000 people in twenty-six countries.

¹⁸ See <http://news.bbc.co.uk/1/hi/world/europe/3603943.stm>.

¹⁹ See for example www.dailymail.co.uk/news/worldnews/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html?ITO=1490.

²⁰ Article 5A, paragraph 2 of the Constitution of Greece states that 'All persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as of the production, exchange and diffusion thereof constitutes an obligation of the State.' See for example www.unhcr.org/refworld/docid/4c52794f2.html.

legally enforceable.²¹ The EU Telecoms Reform Package agreed in 2009 supports high-speed access for ‘all citizens’ throughout the EU.²²

In the UK, surveys suggest the same. In 2009, a survey for the Communications Consumer Panel showed that ‘84 per cent of people agreed that it should be possible for everyone in the UK to have broadband at home, regardless of where they live. Many people already see broadband as essential and even more believe that soon it will be essential for everyone.’ As Communications Consumer Panel Chair Anna Bradley put it:

The tipping point will be when broadband does not just provide an advantage to people who have it, but disadvantages people who do not. Interestingly some people already feel disadvantaged: those who live in not-spots and those who have school-age children but do not have broadband at home.²³

The idea that internet access could be a human right is debatable. Vint Cerf, for example, one of the ‘fathers of the internet’, has suggested that it is not.²⁴ The nature and scale of the discussion over this issue, however, and the reality of the way that the internet is used in practice do suggest that at the very least an inability to access the internet puts people at a significant disadvantage. To be able to participate fully in contemporary life, people need internet access, and so to participate freely in that life, people need the opportunity to act freely on the internet.

1.2 Data and the internet

The internet offers hitherto unheard-of opportunities to gather, analyse, use and store personal data, and it has become the focus of efforts to do all of this.²⁵ The case studies in Chapters 5 to 7 reveal just some of the ways in which this is already happening, and give at least some idea of how this could develop into the future.

²¹ See for example www.bbc.co.uk/news/10461048. Finland not only made internet access a legal right, but specified a minimum speed of access of 1Mbps.

²² See <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491>.

²³ www.communicationsconsumerpanel.org.uk/press-releases/press-releases/post/173-soon-it-will-be-essential-for-everyone-to-have-broadband.

²⁴ See for example www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=0.

²⁵ Each of Cate’s four principles for data growth, set out in Cate (1997, pp. 13–16), applies directly to the Internet. His fourth principle in particular refers to the impact of computer networks.