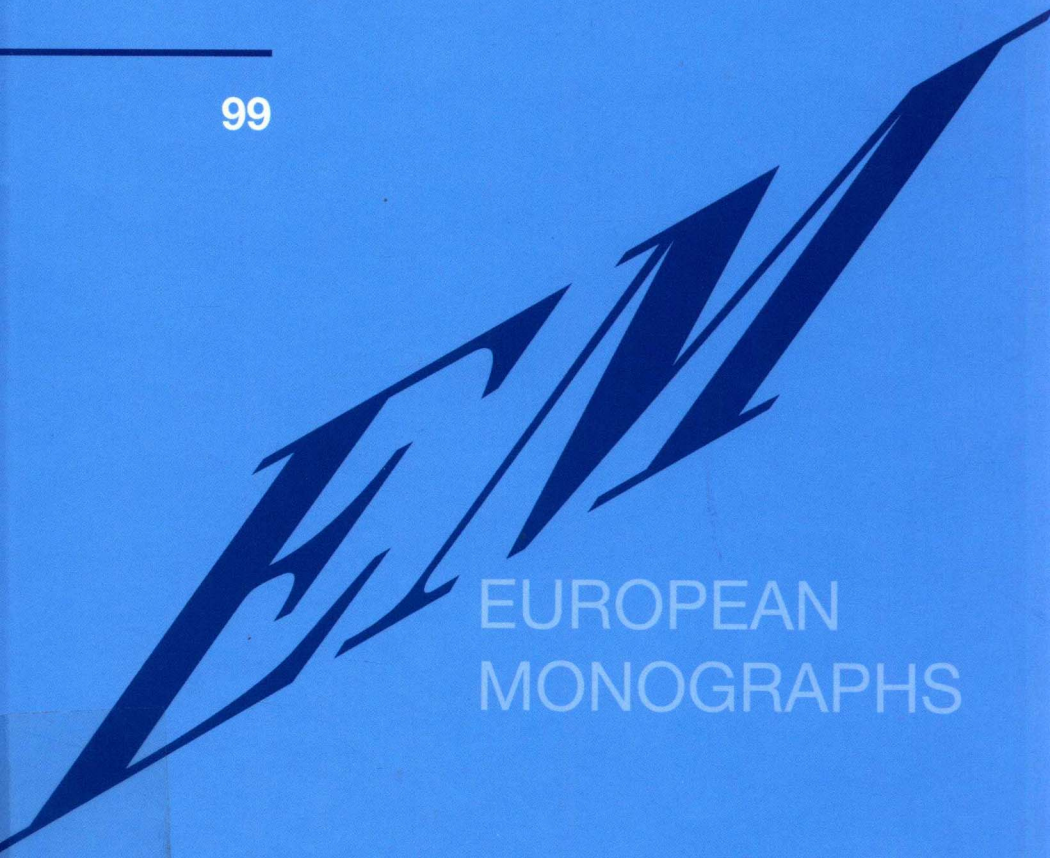
Privacy Limitation Clauses

Trojan Horses under the Disguise of Democracy

Robert van den Hoven van Genderen

99



Wolters Kluwer

Privacy Limitation Clauses

Trojan Horses under the Disguise of Democracy

Robert van den Hoven van Genderen

Published by:
Kluwer Law International B.V.
PO Box 316
2400 AH Alphen aan den Rijn
The Netherlands
Website: www.wklawbusiness.com

Sold and distributed in North, Central and South America by:
Wolters Kluwer Legal & Regulatory U.S.
7201 McKinney Circle
Frederick, MD 21704
United States of America
Email: customer.service@wolterskluwer.com

Sold and distributed in all other countries by:
Turpin Distribution Services Ltd
Stratton Business Park
Pegasus Drive, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom
Email: kluwerlaw@turpin-distribution.com

Printed on acid-free paper.

ISBN 978-90-411-8599-0

e-Book: 978-90-411-8600-3
web-PDF: 978-90-411-8601-0

Printed in the United Kingdom.

Privacy Limitation Clauses

European Monographs Series Set

VOLUME 99

Editor

Prof. Andrea Biondi is Professor of European Law and Director of the Centre of European Law at King's College London

Introduction & Contents/Subjects

As the process of European integration assumes an increasingly complex character, the EU legal system continues to undergo sweeping changes. The European Monographs series offers a voice to thoughtful, knowledgeable, cutting edge legal commentary on the now unlimited field of European law. Its emphasis on focal and topical issues makes the series an invaluable tool for scholars, practitioners, and policymakers specializing or simply interested in EU law.

Objective

The aim is to publish innovative work appealing to academics and practitioners alike. The result is an original and ongoing library of detailed analyses, theories, commentaries, practical guides, and proposals, each of which furthers the cause of meaningful European integration. Cumulatively, the series may be regarded as a 'work in progress' engaged in building a sharply defined representation of law in Europe.

Readership

Academics and practitioners dealing with EU law.

The titles published in this series are listed at the end of this volume.

‘During times of universal deceit, telling the truth becomes a revolutionary act.’

George Orwell

Table of Contents

Chapter 1
Introduction

'The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement!'

William Pitt, English Parliamentarian, 1765

In an era where the behaviour of authorities, industry and the subjects themselves undermine the very essence of privacy, it is time to analyse the source of this behaviour from a legal perspective. We are currently living in an era of 'big data' where governments and others, like Google and Amazon, collect large amounts of data about us, *nolens volens*, just for the sake of possible use in the future, crossing our thresholds without our permission.

National States have the legal and functional power to limit the fundamental rights of individuals in order to protect society for the benefit of the sum of individuals. When they do this, States are responsible for justifying their actions by grounding them in the general principles of law. In this book the reasoning, circumstances and legal justification underpinning these decisions will be scrutinised.

In the twenty-first century we witnessed two notable events, each of a completely different character, which had influential effects on the concept of privacy and the possible limitation of, and intrusion into this right by governments.

First, there was the threat of terror, embodied in the devastating attack on the World Trade Center in New York on 11 September 2001. This event prompted authorities to develop both national and international legal instruments designed to protect national security interests and combat terrorism, but at the same time intrude upon and limit the personal privacy of individuals.

The other event was the revelations by Edward Snowden, starting in 2013 about the ways, means and methods employed by national security agencies (notably the National Security Agency (NSA) of the United States (US) and the Government Communications Headquarters (GCHQ) of the United Kingdom). The so-called

Snowden files raised serious doubt and criticism of the operations of secret (intelligence) agencies.

This latter event made clear that State authorities seriously intrude on privacy, sometimes crossing the line of their legal limitations.

If we still accept that the concept of private property and virtual property, in the sense of personal information, is the source of all integrity, we have to be alert to any intrusion into privacy in the widest sense. Locke already claimed that the State's only reason for existence was its function to protect life, liberty and estate.[1] A fundamental question 300 years ago and still today pertains to how governmental authorities, in the case of fundamental rights, e.g., privacy, should balance the general interests of the State with the inviolability of the interest of the citizens whom they are obliged to protect. Fundamental rights like privacy are recognised in international treaties, e.g., the European Charter, the European Convention on Human Rights (ECHR), the International Covenant for Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR).

Fundamental to every legal system should be the following four principles as presented by the famous Dutch legal scholar Paul Scholten:[2]

1. Personality of the autonomous human being;
2. Limitations of rights only by the justice of the community;
3. Right of equality against the Authority and;
4. The separation between good and evil, the root of all justice.[3]

With regard to the concept of privacy, all of these principles are strongly connected: the right to determine what will be done with one's personal information and to what extent one's personal life is protected should be upheld above those in government; they should be applied on the basis of equality and only restricted in well-defined circumstances. Currently, however, these restrictions tend to be applied on a flexible basis.

Fundamental rights are often restricted in reaction to (perceived) threats of terrorism. The international human rights treaties do contain exceptions that allow sovereign States to restrict fundamental rights, but only if specific circumstances justify it. These circumstances are often ambiguous and are certainly not clearly defined in either national or international regulations.

The aim of this book is to analyse the tension between the fundamental right to privacy and the constraints under which these exceptions are justified. The specific areas studied are:

1. Locke's (1690) main concept *Property* covers these three concepts: '(...) to preserve his Property, that is, his Life, Liberty and Estate (...).' (Second Treatise, § 87). The US Constitution is inspired by Locke, but uses another triad that includes property, viz. in the Fifth Amendment 'nor be deprived of life, liberty or property' and the Fourteenth Amendment 'nor shall any state deprive any person of life, liberty or property.' John Locke, *Two Treatises of Government*, (first published 1690, Penguin 1987) and John Locke, *Two Treatises of Government*, Ed Thomas Hollis (London: A. Miller *et al.*, 1794).
2. Scholten 1974.
3. Although this principle is essential, the elaboration will be consized.

(1) data protection regulations;
(2) the regulations on interception and retention of personal data in the telecommunication sector;
(3) money laundering; and
(4) the strategies used to protect national security against terrorist activities.

These areas will be commented from a predominantly European perspective.

§1.01 TYPES OF PRIVACY AND DIFFERENT ROLES

Defining privacy is one of the most intractable problems in privacy studies.[4] Perhaps even more difficult is the weighing of the value of privacy against that of public interest.[5] From a socio-philosophical perspective, privacy can also be defined as a 'control right' to which I concur:

> A privacy right is an access control right over oneself and to information about oneself. Privacy rights also include a use or control feature—that is, privacy rights allow me exclusive use and control over personal information and specific bodies or locations.[6]

The fundamental right to privacy, in the sense of non-interference by government, is protected by international and national law. In its essence, the elements of privacy are based upon the non-interference principle of Article 8 of the ECHR: Everyone has the right to respect for his privacy and family life, his home and his correspondence.

Although the protection of privacy, family life and communications is secured by Article 7 of the Charter of Fundamental Rights of the European Union,[7] the European Union (EU) specifies, in Article 8, the protection and control of personal data. By specifying protection and control over personal data, the Charter stresses the importance of data protection. De Hert and Gutwirth explain the differentiation between privacy and data protection as:

> For us privacy is an example of a 'tool of opacity' (stopping power, setting normative limits to power), while data protection and criminal procedure can be mainly -not exclusively- seen as 'tools of transparency' (regulating and channelling necessary/reasonable/legitimate power).[8]

A substantial aspect of the willing or unwilling intrusion of privacy these days consists of processing of personal data of individuals, the so-called data subjects.

4. Reidenberg 1992.
5. *See* Arendt 1949, pp. 69-71, in Gregory J.Walters, 'Privacy and Security: An Ethical Analysis', *Computers and Society* 2001, p. 9.
6. *See* Adam Moore, 'Defining Privacy', *Journal of Social Philosophy,* no. 3, pp. 411-428, Fall 2008, p. 414.
7. Charter of Fundamental Rights of the European Union (2010/C 83/02).
8. Gutwirth, Serge & De Hert, Paul. 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law.* Antwerpen-Oxford: Intersentia 2007 pp. 61-104.

Individuals have a strong urge to be in control of their personal information under a variety of circumstances. There is such an abundance of data, which is used in both social and commercial networks, that control by the data subject of the processing of his/her own data is almost impossible. Governments here possess and occupy two different, janus-faced roles: on the one hand, the government is the defender of privacy as a privacy regulator and authority; on the other hand, the government may legitimately 'attack' privacy, as in the Department of Justice or the Ministry of Interior Affairs. The result is as stated by the prominent scholar/theorist Westin in 'Privacy and Freedom' in 1970:

> Drawing the line between what is proper privacy and what becomes dangerous 'government secrecy' is a difficult task.[9]

In criminal investigations, and certainly for the protection of national security, the use of personal data is maximised within the boundaries of the law. There is a tendency by governmental authorities to hold control over information and personal data streams. The use of personal information can then go beyond the originally-defined purpose of processing of this personal information, what can be called 'function creep.' This can result in the excessive use of personal information by authorities, insofar as it may injure the informational sovereignty of the data subject by 'function creep'.[10]

In this book, privacy is referring to the right of natural persons to control information about themselves and the non-interference by government. This definition is based on the German constitutional right of human dignity, leading to the concept of informational self-determination as created by the German Constitutional Court, 'Bundesverfassungsgericht' in 1983.[11] Privacy may entail a right to a lack of disclosure of personal information but at the very least also contains a right to selective disclosure of personal information.[12] The natural person should be considered the master, sovereign over his/her privacy. The aspect of information rights to inform natural

9. Westin 1970, p. 49.
10. An example in the Netherlands of 'function creep' in this respect is the extension of the use by governmental agencies concerning the electronic registration and storage of license plate registrations within the electronic number plate car registration (ANPR). This information can be used by police, the Ministry of Finance, Social Security an Intelligence Agencies. In these files different governmental and non-governmental organisations will have access to sensitive personal data Different agencies, justice, tax authorities, social security and national intelligence can exchange these data amongst each other without a transparent control mechanism. The privacy regulator has issued guidelines how to apply this competence.
11. Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, Az.: 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/8. *See also*: Gerrit Hornung & Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination', *Computer Law & Security Review*, no. 1, 2009, pp. 84-88, citing: it would be contradicting the constitutional guarantee of human dignity for the government to claim the right to compulsorily register and index an individual's complete personality even in the anonymity provided by a statistical census, since the individual would be treated as an object accessible to an inventory in every way.'
12. McCloskey, Henry J. 'Privacy and the Right to Privacy.' *Philosophy* Vol. 55, 1980, p. 22.

persons/subjects of processing personal information in governmental and criminal files as such will not be the subject of this book.[13]

Data protection is a separated aspect of the protection of the personal sphere on a legal basis but should be included as an aspect of privacy. This is described by Gellert and Gutwirth as follows:

> Law distinguishes between privacy and data protection. Law understands the legal right to privacy as protecting the intimacy as well as the autonomy and self-determination of citizens, whereas data protection is seen as a legal tool that regulates the processing of personal data. Ultimately, both rights are considered as instrumental tools in order to protect the political private sphere, which hallows the autonomy and determination of the individual.[14]

[A] Limitation of Privacy as a Sovereign Right of Society

Central in this book is Article 8 of the ECHR.

Article 8 of the ECHR provides the right for one's private and family life, home and correspondence, to be respected, subject to certain restrictions that are 'in accordance with law' and 'necessary in a democratic society'. Essentially, the ECHR protects individuals from non-interference unless there are legitimate exceptions provided by the relevant authorities.

In the comments and court decisions on Article 8 of the ECHR, it is recognised that, essentially, the right to respect for one's private and family life, as well as his home and correspondence, entails that State authorities must refrain from interfering in personal privacy, whenever, wherever. Although Article 8(2) places some limits on Article 8(1), States must guarantee this right to privacy to their citizens and indeed protect it.[15] That guaranteeing in Article 8(1) should be the core of any legal instrument defining privacy or personal data protection.

Moreham in his article on the respect for private life in the ECHR derives even more rights from Article 8 ECHR, including:

(1) the right to be free from interference with physical and psychological integrity;
(2) the right to be free from unwanted access to and collection of information;
(3) the right to be free from serious environmental pollution;

13. I refer to transparency of that use, in the sense of control, review, objection and erasure of personal information.
14. Gellert & Gutwirth, *Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment,* Prescient. FP 7 project March 2013.
15. Article 8(2) of the ECHR states:

> 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.

(4) the right to be free to develop one's personality and identity; and
(5) the right to be free to live one's life in a manner of one's choosing.[16]

Indentifiable aspects in the case law and commentary of the European Court of Human Rights (ECtHR) reveal still further complementary elements falling under Article 8 of the ECHR, such as:

(1) those identifiable elements are gathered by government and business files; or
(2) data gathered by security services or other organs of the State by searches and seizures; and
(3) surveillance of communications and telephone conversation.[17]

The surveillance activities have been under scrutiny in the 2015 and 2016 cases by the ECtHR in the Zakharov cases.[18] Based on the last case there is a tendency to add to this list: all digital traces that reveal the whereabouts or activities of a natural person as the traffic and location data. In the end the common aspect is, they all are data considered leading to the identification of a data subject.

Privacy is increasingly challenged in case law in the face of changing socio-cultural and technological circumstances. At the same time, privacy is becoming ever more limited by governments facing unstable political circumstances and increased technological capabilities. Unsurprisingly then, it is impossible to define any absolute right to privacy unequivocally. The threat of terrorism is increasingly stimulating the intrusion of governments on personal information. After the Charlie Hebdo incident in January 2015, France passed its controversial 'surveillance Bill', giving French intelligence and police increasing its surveillance competences. After the second wave of terrorist attacks in November of that same year the determination of those inquisitive regulations is certified.

It also must be kept in mind that fundamental rights are limited by the rights of other legal subjects and by regulations deemed necessary for the protection of society. The limits of the non-absolutism of privacy can be compared with the theoretical concept described by Scholten where the fundamental rights are never considered absolute. As early as 1935, Scholten stated that, although fundamental legal principles may seem undisputed, they find their limitation in other legal principles. Scholten builds further on the observation of Kant who bases his Doctrine of Right on the fact that there is only one innate right: 'Freedom (independence from being constrained by

16. Nicole A. Moreham, 'The Right to Respect for Private Life in the European Convention on Human Rights: A Reexamination', *European Human Rights Law Review*, no. 1, 2008, pp. 44-79.
17. Referring to case law of the ECtHR: *Weber and Saravia v. Germany* and *Valenzuela Contreras v. Spain*. Also *Key case-law issues. The concepts of 'private and family life'. Article 8 – Right to respect for private and family life*, 2007 by Antonella Galetta & Paul De Hert, *Utrecht Law Review*, no. 1, January 2014, p. 57.
18. *Zakharov v. Ukraine* (Application no. 26581/06) (final 7 April 2016).