

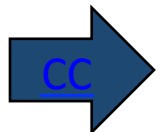
**„True Fiction: Die Digitalisierung unseres Alltags“
24. bis 26. September 2015 Stiftung Leucorea
Lutherstadt Wittenberg**

**Informationsethische, -rechtliche, -
ökonomische und –politische Aspekte von
Privatheit in elektronischen Räumen**

**Eine private oder eine soziale
Herausforderung**



**Rainer Kuhlen
Fachbereich Informatik und
Informationswissenschaft
Universität Konstanz**



Wasser

Dürre



politisch korrekt?

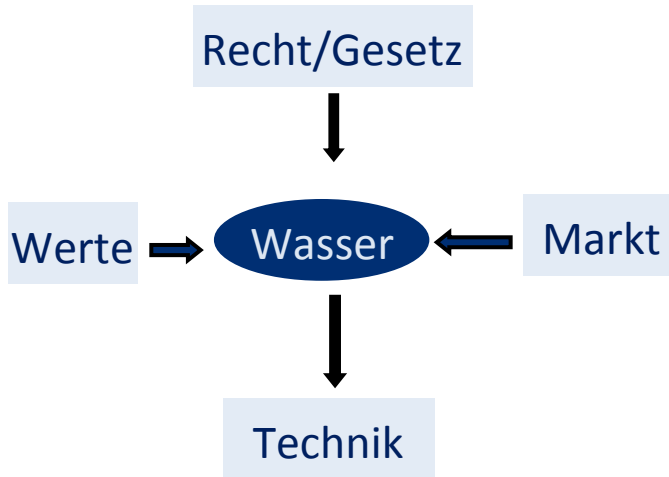
ethisch angreifbar?



Regulierungsformen - Institutionalisierungsformen



Regulierungsformen - Institutionalisierungsformen



res nullius?

nein

privat?

nein

öffentlich?

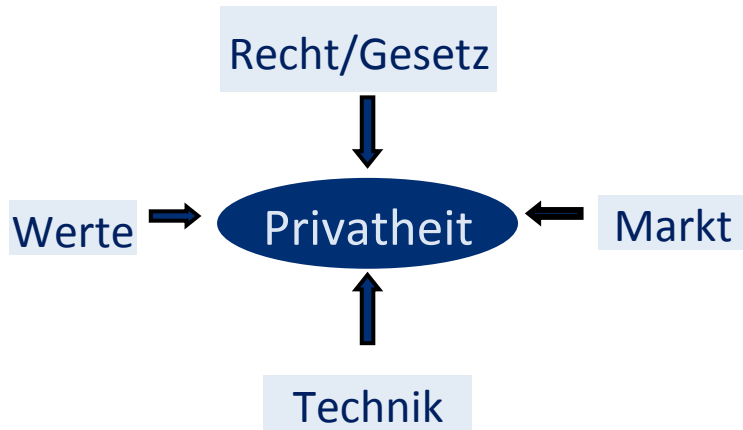
nein

gemeinschaftlich?

ja

ein Commons?

Regulierungsformen - Institutionalisierungsformen



res nullius?

nein

privat?

ja - aber

öffentlich?

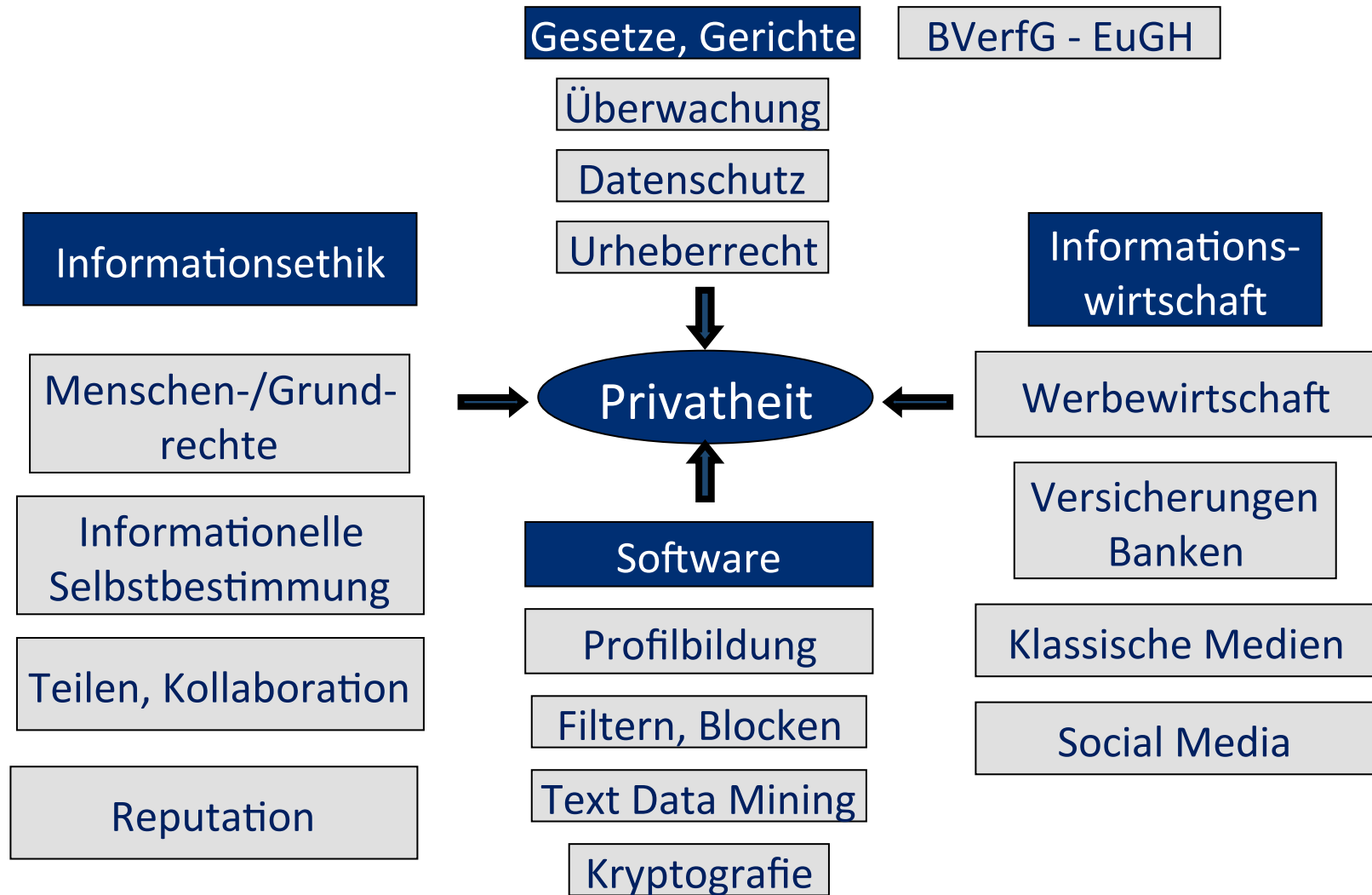
nein - aber

gemeinschaftlich?

nein - aber

ein Commons?

Regulierungsformen - Institutionalisierungsformen



**Was war, ist, wird Privatheit /
privacy ?**

Ein Recht

the right to be let alone

“The Right to Privacy”

Warren and Brandeis

Harvard Law Review.

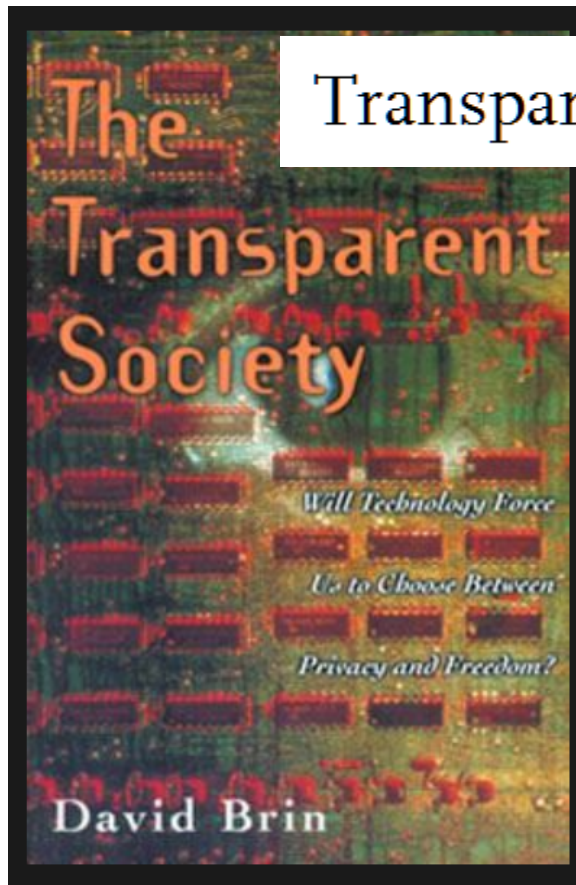
Vol. IV December 15, 1890 No. 5

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary **from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.**

...

and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession -- intangible, as well as tangible.

Privatheit / privacy obsolet? Ein Überbleibsel
des bürgerlichen 19. Jahrhunderts?



Transparency is the trick to protect privacy

by David Brin
Perseus Books, 1998

I'd been writing about the issues of transparency, security and privacy for several years before the publication of **The Transparent Society**.

In this book (and in *all* my writings) I emphasize **openness and transparency** as a good general policy for the era ahead, when a myriad pitfalls and unexpected dangers may loom suddenly out of the future. Above all, openness is freedom's best defense.



Privatsphäre als persönlicher Raum, der sich sicher weiß vor fremden Blicken, ist praktisch tot. Schuld ist das Internet.

Datenschutz ist bestenfalls Hinauszögern des Unausweichlichen, schlimmstenfalls ein Kampf gegen Windmühlen.

Wichtiger ist die Frage, wie wir unser Leben ohne die Sicherheiten der Privatsphäre lebenswert machen können.



Informationelle Selbstbestimmung

BVerfGE 65,1 – Volkszählung

1983

Leisätze:

- 1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*
- 2. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.*

Informationelle Selbstbestimmung

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“ (BVerfGE 61, 1, C II 1a)

Informationelle Selbstbestimmung

In elektronischen Wissens- und Informationswelten

mündiger, selbstbestimmter Umgang mit Wissen und Information.

Recht und Fähigkeit eines jeden Individuums, seine privaten, professionellen und öffentlichen Geschäfte (Handlungen) **informationell abgesichert** abwickeln zu können

Informationelle Selbstbestimmung

Reguliert werden können Informationsgesellschaften **nur über**
informationell gebildete und informationell autonome
Menschen.

Ansonsten bestimmen der dynamische **mediale technische**
Determinismus und die Interessen der Märkte, wie wir leben
sollen.

Bundesdatenschutzgesetz (BDSG)

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

orientiert sich am Prinzip der informationellen Selbstbestimmung und an den allgemeinen Persönlichkeits-/Grundrechten

und sieht als primäre Lösung das “informed consent model” (ICM) an

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Prinzip bisheriger Privatheit-Regulierungen

“informed consent model” (ICM)

“customary notice-and-choice approach” (USA)

ICM beruht auf zwei plausiblen Annahmen:

“(1) that privacy has to do with the ability of data subjects to control information about them, and
(2) that people have very different privacy preferences.” (p.3)

“informed consent is necessary to obtain legitimacy and it is sufficient to obtain legitimacy. With informed consent, any information collection and use practice is legitimate. Without it, no information collection and use practice is legitimate.”

“Informed consent makes an information practice legitimate.” (10))



Recht auf Vergessen

Court of Justice of the European Union

PRESS RELEASE No 70/14

Luxembourg, 13 May 2014

Judgment in Case C-131/12

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos,
Mario Costeja González

Press and Information

An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties

Thus, if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results

„Individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them. This applies where information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing.“ Dieses Recht auf Vergessen gilt nicht absolut: „, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media (para 85 of the ruling).

http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

Privacy as property - Part V: Democratic Process and Nonpublic Politics

Social Research, Spring, 2002 by Lawrence Lessig

<http://www.englishdiscourse.org/lessig.html>

In a recent essay, Harvard professor Jonathan Zittrain argued that there is no conceptual difference between the "privacy problem" and the "copyright problem" (Zittrain, 2000).

Both, he argued, are examples of data getting out of control. In the context of privacy, it is personal data over which the individual loses control--medical records, for example, that find their way to a drug company's marketing department; or lists of videos rented, that before the protections granted by Congress, found their way to a Senate confirmation hearing. The problem with privacy is that private data flows too easily--that it too easily falls out of the control of the individual.

So understood, Zittrain argued, the problem of copyright is precisely the same. It too is a problem of data getting out of control.

Menschenrecht



Generalversammlung

Verteilung: Allgemein
10. Dezember 1948

Dritte Tagung

Resolution der Generalversammlung

217 A (III). Allgemeine Erklärung der Menschenrechte

Artikel 12 - Schutz der Freiheitssphäre des Einzelnen

Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden. Jeder Mensch hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Anschläge.

Zum Privatleben gehört nach heutiger Auffassung in erster Linie die **Identität** (u.a. Name, Kleidung, Haartracht, Gefühle und Gedanken), die **Integrität** (was etwa eine medizinische Behandlung gegen den Willen der Betroffenen ausschliesst), die **Intimität** (wie etwa die Geheimhaltung privater Eigenschaften und Handlungen, der Schutz des eigenen Bildes vor Veröffentlichung oder der Schutz vor Weitergabe personenbezogener Daten), die **Kommunikation** (z.B. die Aufnahme und Entwicklung von Beziehungen zu anderen Leuten) und die **Sexualität** (allerdings darf hier der Staat zum Schutze bestimmter Personengruppen, etwa von Kindern, Einschränkungen wie z.B. ein Mindestalter vorschreiben).

Europäische Menschenrechtskonvention

Abschnitt I - Rechte und Freiheiten (Art. 2 - 18)

Artikel 8

Recht auf Achtung des Privat- und Familienlebens

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

Große Texte



Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Strasbourg, 28.1.1981

Aus der Präambel

in der Erwägung, daß es angesichts des zunehmenden grenzüberschreitenden Verkehrs automatisch verarbeiteter personenbezogener Daten wünschenswert ist, den Schutz der Rechte und Grundfreiheiten jedes Menschen, vor allem das Recht auf Achtung des Persönlichkeitsbereichs, zu erweitern;

in Anerkennung der Notwendigkeit, die grundlegenden Werte der Achtung des Persönlichkeitsbereichs und des freien Informationsaustausches zwischen den Völkern in Einklang zu bringen

In diesem Übereinkommen:

bedeutet "personenbezogene Daten" jede Information über eine bestimmte oder bestimmbare natürliche Person ("Betroffener") (Art. 2)

<http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm>

CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION

Große Texte

(2000/C 364/01)

Artikel 7

Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8

Schutz personenbezogener Daten

- (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
- (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
- (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

The Madrid Resolution

1 Purpose

The purpose of this Document is:

- a. To define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data; and
- b. The facilitation of the international flows of personal data needed in a globalized world.

Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data

http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

Global Privacy and Cybersecurity Law Updates and Analysis

<https://www.huntonprivacyblog.com/tag/madrid-resolution/>

Mit laufender Information zur Übernahme der Madrid Resolution durch verschiedene Länder.

The Madrid Resolution

Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data

http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

■ Principle of lawfulness ■ and fairness

- 1. Personal data must be fairly processed, respecting the applicable national legislation as well as the rights and freedoms of individuals as set out in this Document and in conformity with the purposes and principles of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.
- 2. In particular, any processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair.

■ Purpose specification ■ principle

- 1. The processing of personal data should be limited to the fulfilment of the specific, explicit and legitimate purposes of the responsible person.
- 2. The responsible person should not carry out any processing that is non-compatible with the purposes for which personal data were collected, unless he has the unambiguous consent of the data subject.

Regelt es der Markt?

Privacy no longer a
"social norm"

People have really
gotten comfortable
not only sharing more
information and
different kinds, but
more openly and with
more people

That social norm is just
something that has
evolved over time.



Photograph: Eric Risberg/AP Eric Risberg/ASSOCIATED PRESS

Klage gegen Facebook: EuGH prüft Datenschutzregeln amerikanischer Konzerne



REUTERS

Datenschutz-Aktivist Max Schrems (Archiv): Hat gegen Facebook geklagt

<http://www.spiegel.de/netzwelt/netzpolitik/facebook-versus-max-schrems-aktivist-zieht-vor-eugh-a-1025129.html>

Vor dem Wiener Landgericht im Juli 2015 noch abgewiesen

Klage gegen Facebook: EuGH prüft Datenschutzregeln amerikanischer Konzerne

Dienstag, 24.03.2015

Der Datenschutz-Aktivist Max Schrems hat mit einer Klage gegen erreicht, dass sich der Europäische Gerichtshof (EuGH) ab Dienstagvormittag mit den Datenschutz-Regeln amerikanischer Firmen beschäftigt. Konkret geht es um die Frage, inwieweit europäische Tochterfirmen von Konzernen wie Facebook und Google die EU-Grundrechtecharta zum Schutz personenbezogener Daten beachten müssen.

Schrems hatte von Facebook eine Herausgabe aller über ihn gespeicherten Informationen verlangt. Von der Europa-Zentrale im irischen Dublin bekam er 2011 mehr als 1200 Druckseiten Material zugeschickt, auf denen sich auch längst gelöschte Daten fanden.

Facebook speichert die Daten europäischer Nutzer auf seinen Servern in den USA. Dem Unternehmen wird vorgeworfen, unter anderem die NSA bei Überwachungsprogrammen wie Prism unterstützt zu haben, zum Beispiel per Zugriff auf Nutzerdaten. Facebook bestreitet diese Vorwürfe.

Facebook-Gutachten

David schlägt Goliath k.o.

Was der Generalanwalt Yves Bot im Verfahren von Max Schrems gegen Facebook vor dem Europäischen Gerichtshof vorschlägt, ist ein Hammer. Der globale Datenhandel würde neu organisiert, die NSA hätte das Nachsehen. Noch ist es nicht soweit. Ein Kommentar.

23.09.2015, von MICHAEL HANFELD

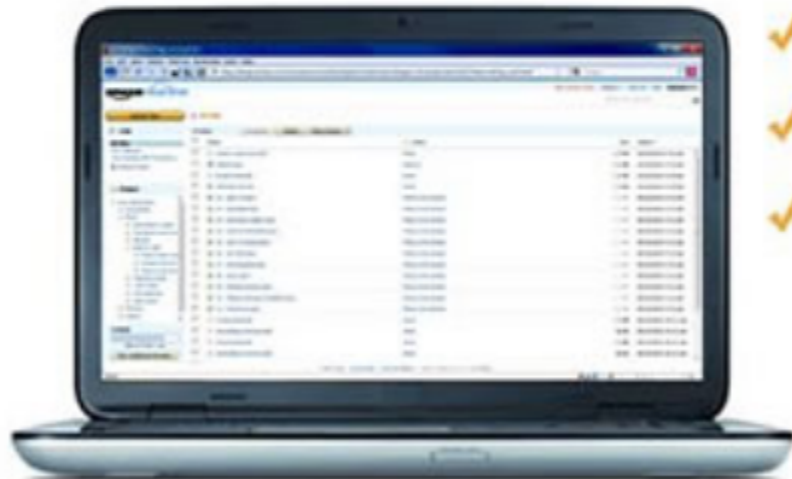
„Server in den Vereinigten Staaten, sagt Bot, seien für die Daten von EU-Bürgern kein „sicherer Hafen“. Sie seien nicht sicher vor dem Zugriff der Geheimdienste und dürften dort folglich nicht gelagert werden. Der „Safe Harbor“-Status, der amerikanischen Unternehmen zugebilligt werde, sei gegenstandslos.“

<http://www.faz.net/aktuell/feuilleton/medien/facebook-gutachten-des-eugh-leitet-zeitenwende-ein-13819102.html>

So auch jetzt das Urteil des EuGH vom 5.10 <http://www.spiegel.de/netzwelt/netzpolitik/europaeischer-gerichtshof-erklaert-safe-harbor-abkommen-fuer-ungueltig-a-1056366.html>

Introducing **amazon** cloud drive

Because Who Needs Privacy?



- ✓ **5 GB** of free online storage **for ~~our~~ your files**
- ✓ Unlimited access from any computer **we own**
- ✓ Never worry about losing your files again **because we'll keep an eye on 'em.**

DOES THIS WORK FOR YOU?

Amazon.com Privacy Notice

Last updated: March 3, 2014. To see what has changed, [click here](#).

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

- [What Personal Information About Customers Does Amazon.com Gather?](#)
- [What About Cookies?](#)
- [Does Amazon.com Share the Information It Receives?](#)
- [How Secure Is Information About Me?](#)
- [What About Third-Party Advertisers and Links to Other Websites?](#)
- [Which Information Can I Access?](#)
- [What Choices Do I Have?](#)
- [Are Children Allowed to Use Amazon.com?](#)
- [Does Amazon.com Participate in the Safe Harbor Program?](#)
- [Conditions of Use, Notices, and Revisions](#)
- [Examples of Information Collected](#)

Prinzip bisheriger Privatheit-Regulierungen

“informed consent model” (ICM)

“informed consent is necessary to obtain legitimacy and it is sufficient to obtain legitimacy. With informed consent, any information collection and use practice is legitimate. Without it, no information collection and use practice is legitimate.”

“Informed consent makes an information practice legitimate.” (10))

Ohne IC ist keine Verwendung der Daten legitim.

Beispiel für Privatheitgarantie

U.S. Department of Health, Education and Welfare (HEW)

- 1) Im Anwendungsbereich oder in einem System darf es kein geheimes Datensammelsystem geben;
- 2) eine Person muss in der Lage sein, welche Information über sie im System existiert und für welchen Zweck sie verwendet wird;
- 3) eine Person muss verhindern können, dass Informationen, die sie für einen bestimmten Zweck freigegeben hat, für andere, ihr unbekannte Zwecke verwendet wird.

Realisiert meistens durch Offenlegung von „Internet privacy policies“.

Ist Offenlegung von „Internet privacy policies“ die Lösung?

in der Praxis kaum gelesen

sehr lang und trotzdem wenig informativ

Kostenaufwand zu lesen und zu verstehen einfach zu hoch.

i. .d.R. nur binäre Entscheidung – ja oder kein Service

Ist Sicherung von Privatheit weniger ein privates, persönliches, als
ein soziales und politisches Problem?

Offenlegung von „Internet privacy policies“ ist keine Lösung?

Am Gravierendsten ist das Problem, dass eine Person gar nicht mehr einschätzen bzw. in Erfahrung bringen kann, welche Daten über sie gesammelt oder für welche Zwecke diese dann genutzt werden.

„It is no longer reasonable to expect a typical Internet user to understand what information is collected about him or her online, what can be inferred from that information, and what can be done with the profiles and analytics based on that information. In this context, relying on informed consent to prevent information harms would be similar to letting people decide for themselves what level of exposure to toxic substances they would accept in the workshop or the environment.“ (McCarthy, 4)

Offenlegung von „Internet privacy policies“ ist keine Lösung?

Am Gravierendsten ist das Problem, dass eine Person gar nicht mehr einschätzen bzw. in Erfahrung bringen kann, welche Daten über sie gesammelt oder für welche Zwecke diese dann genutzt werden.

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“ (BVerfGE 61, 1, C II 1a)

Wird das nicht die Gesellschaftsordnung nicht zuletzt der sozialen Medien?

Denn in der Tat weiss man nicht mehr, wer, was wann Gibt es dann also kein Recht auf informationelle Selbstbestimmung? – ein Recht, das prinzipiell nicht eingelöst werden kann – ist kein Recht mehr.

Ist Offenlegung von „Internet privacy policies“ die Lösung?

Kaum

Immer mehr Privatheitsverletzungen geschehen durch „negative privacy externalities“ (MacCarty)
auch “indirect privacy concerns” genannt (Luc Wathieu

Gerade in sozialen Netzwerken sind durch persönliche Daten (z.B. Bilder von einer Party), die jemand nach dem ICM freigibt, oft Dritte betroffen, die gar nicht erfahren, dass einige ihrer durch die Freigabe mitbetroffenen Daten nun frei genutzt werden und schon gar nicht erfahren, wer für welche Zwecke diese Daten nun nutzt.





Konsequenzen von negative privacy externalities (NPE)

Informationelle Selbstbestimmung wird dadurch eingeschränkt, dass durch die Annahme der Bedingungen einer „Internet privacy policy“ durch eine Person A weitere Personen betroffen sind, die z.B. in einem Bild mit vorkommen und die zum einen von dieser Nutzung durch Dritte gar nichts erfahren geschweige denn ihr zugestimmt hätten.

In der komplexen Informationswelt des Internet ist es schlichtweg nicht mehr möglich, individuelle Privatheit im Sinne einer autonomen Verfügung/Selbstbestimmung durch eigene Initiative und dann auch noch mit Vollständigkeitsanspruch zu sichern.

Das Privatheits-Problem wird von einer individuellen auf eine soziale Ebene verschoben.

Privatheit ist nicht in erster eine Datenschutzherausforderung sondern ein Informationsproblem.

Privatheit ist nicht nur eine Datenschutzherausforderung
sondern auch und vor allem ein Informationsproblem



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario



Welcome to the IPC website!

Welcome to the Office of the Information and Privacy Commissioner of Ontario. Since January 1, 1988, the IPC has acted independently of government to uphold and promote open government and the protection of personal privacy in Ontario. Here you will find numerous resources to assist in protecting your privacy and accessing information. Please contact us at info@ipc.on.ca with any questions.

Brian Beamish

Learn more about Commissioner Brian Beamish.

Transparency, Privacy and the Internet: Municipal Balancing Acts



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

PROMOTING ACCESS & PROTECTING PRIVACY
FINDING THE BALANCE

[Home](#) | [Government of NL](#) | [House of Assembly](#) | [Search](#) | [Contact Us](#) | [Follow Us on Twitter](#)

Privatheit ist nicht nur eine Datenschutzherausforderung
sondern auch und vor allem ein Informationsproblem



information
and privacy
commission
new south wales



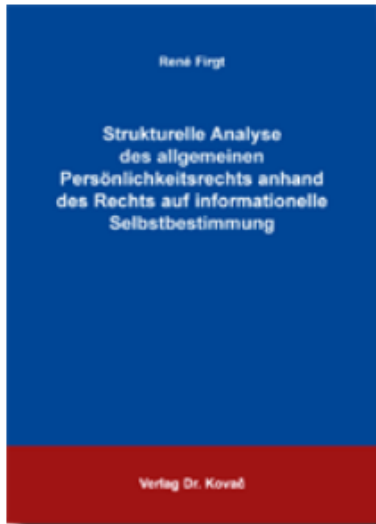
OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.



Office of the
Saskatchewan Information
and Privacy Commissioner

Informationeller Selbstbestimmung als Sicherung von
Persönlichkeitsrechten reicht nicht aus – eher zu sichern
durch ein Bündel von Rechten.



René Firtg

**Strukturelle Analyse des allgemeinen
Persönlichkeitsrechts anhand des
Rechts auf informationelle
Selbstbestimmung**

Schriften zum Persönlichkeitsrecht, Band 12

Hamburg 2015, 352 Seiten

ISBN 978-3-8300-8344-3

Dissertation
Fernuniversität
Rechtswiss Fak
Hagen
WS 2014/15

Das Buch analysiert und strukturiert die modernen Kommunikationsprozesse. All diese Prozesse lassen personenbezogene Informationen entstehen. Es werden die Wirkungszusammenhänge zwischen diesen Informationen und der aus ihrer Verwendung entstehende Bedrohung der persönlichen Freiheit dargestellt. **Es wird deutlich, dass das Recht auf informationelle Selbstbestimmung dieser amorphen Bedrohungslage nicht gerecht werden kann. Die Allgegenwärtigkeit von Informationen in verschiedenen Lebensbereichen kann zu ganz unterschiedlichen Beeinträchtigungen der Freiheitswahrnehmung des Einzelnen führen. Ein zentral im Allgemeinen Persönlichkeitsrecht verankerter Schutz ist aber aufgrund seiner Konstruktion als Auffanggrundrecht nur subsidiär heranzuziehen.** Stimmiger wäre es, die einzelnen Freiheitswahrnehmungen um die dabei entstehenden Informationen zu erweitern. **Informationsschutz würde dann durch die verschiedenen Grundrechte gewährleistet.**

Es geht um den Umgang mit Informationen, die aus
personenbezogenen Daten abgeleitet und damit
handlungsrelevant werden

Damit kommt die Informationswissenschaftliche
pragmatische Sicht auf Information ins Spiel

Information ist handlungsrelevantes interessengeleitetes
Wissen

Im Kontext von Privatheit

personenbezogene Daten sind nicht schützenswert an
sich, sondern erst indem sie für jemand zur Information
werden

personenbezogene Daten sind nicht in jedem Fall
schützenswert

Im Kontext des ICM und der
negative privacy externalities

Prinzip bisheriger Privatheit-Regulierungen

“informed consent model” (ICM)

“customary notice-and-choice approach” (USA)

ICM beruht auf zwei plausiblen Annahmen:

“(1) that privacy has to do with the ability of data subjects to control information about them, and

(2) that people have very different privacy preferences.” (p.3)

“informed consent is necessary to obtain legitimacy and it is sufficient to obtain legitimacy. With informed consent, any information collection and use practice is legitimate. Without it, no information collection and use practice is legitimate.”

“Informed consent makes an information practice legitimate.” (10))

personenbezogene Daten sind nicht in jedem Fall
schützenswert

Im Zentrum sollte nicht kontrollierte Offenlegung stehen, weil dadurch zu umfänglich negative privacy externalities entstehen, sondern die Bewertung der Folgen der Informationssuche: „Policymakers need to evaluate directly the outcomes of information use, and not focus solely on creating an ideal information collection process.” (MacCarthy, 44)

Erweiterung des bislang dominierenden ICM durch ein „unfairness framework“

Es beruht darauf, dass eine individuelle Zustimmung zu einer Policy nicht mehr die Verwendung der Daten erlaubt, wenn der durch „negative privacy externalities“ entstandene Schaden sehr groß ist.

Mac Carthy führt dafür 3 Kategorien ein:

1. “Impermissible collection and use of information is so harmful that even with data subject consent it should not be permitted.”
2. “Public benefit use of information is so important that it should be allowed even without data subject consent.”
3. “In between lies the realm of consent, where information can be collected and used subject to an opt-in or opt-out regime. An opt-in regime would make sense for the information uses that are closer to the impermissible uses and opt-out would be adopted for the information uses closer to the public benefit use.”

Fazit

Schutz von Privatheit ist eine hyperkomplexe Herausforderung und Gegenstand verschiedener Regulierungsinstanzen mit durchaus heterogenen Interessen

Die Komplexität des Problems darf aber nicht dazu führen, das Konzept von Privatheit auf die Müllhalde der Geschichte zu werden

Das persönlichkeitsrechtsbezogene Konzept der informationellen Selbstbestimmung reicht als Schutz von Privatheit nicht aus

Ebenso reicht das bislang dominierende “informed consent model” (ICM) nicht aus, nicht zuletzt wegen der negative privacy externalities.

Nicht zuletzt wegen der Heterogenität der Schutz- und Nutzungsinteressen von personenbezogenen Daten ist ein Wandel von der statischen Datensicht auf eine dynamischen Informationsicht erforderlich.

Fazit

Privatheit in elektronischen Umgebungen unter Berücksichtigung der verschiedenen Regulierungsinstanzen (Recht, Markt, Technologie, Ethik) ist eine zentrale Herausforderung an die Informationswissenschaft

Vielen Dank für Ihre Aufmerksamkeit!

Mehr Fragen als Antworten



Namensnennung-Weitergabe unter gleichen Bedingungen 2.0 Deutschland

Sie dürfen:



das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen



Bearbeitungen des Werkes anfertigen

Zu den folgenden Bedingungen:



Namensnennung. Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen (wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt).



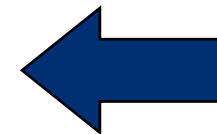
Weitergabe unter gleichen Bedingungen. Wenn Sie dieses Werk bearbeiten oder in anderer Weise umgestalten, verändern oder als Grundlage für ein anderes Werk verwenden, dürfen Sie das neu entstandene Werk nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen. Am Einfachsten ist es, einen Link auf diese Seite einzubinden.
- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Die gesetzlichen Schranken des Urheberrechts bleiben hiervon unberührt.

Die Commons Deed ist eine Zusammenfassung des **Lizenzvertrags** in allgemeinverständlicher Sprache.

CC als Möglichkeit,
informationelle Autonomie/
Selbstbestimmung von Autoren
zurückzugewinnen



im Rahmen des
Urheberrechts, aber mit
Verzicht auf exklusive
Verwertungsrechte