INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES
SECOND EDITION
EDITED BY
JAMES D. WRIGHT

From Busch, A., 2015. Internet and Privacy. In: James D. Wright (editor-in-chief), International Encyclopedia of the Social & Behavioral Sciences, 2nd edition, Vol 12. Oxford: Elsevier. pp. 593–599.
ISBN: 9780080970868

Internet and Privacy

Andreas Busch, Georg-August-Universität Göttingen, Göttingen, Germany

Abstract

The issue of informational privacy has grown in political prominence and importance as use of the Internet has spread around the globe. Economic interests base business models on users' indirect payment with personal data; criminals engage in fraudulous 'identity theft'; and private and public sector surveillance is conducted in order to increase security. But attempts at protecting privacy through regulation on both national and international levels face substantial difficulties which relate to both technical and political causes.

Introduction

The Internet has become an indispensable feature of everyday life in the first decade of the third millennium. No longer confined in use to experts but user-friendly enough to require little training, the Internet is now available not only to citizens in developed countries (where around 80% now have access), but will be to almost 3 billion people around the world by the end of 2014 (40% globally; 32% in developing countries). The contribution to economic growth and dynamism undoubtedly counts among the beneficial consequences of this development. But worries about the negative effects that may accompany this have also emerged, for in a world where users are continuously 'online,' privacy can be endangered if their every move and request can be traced, stored, searched, and potentially forever replicated. Threats to privacy can come from various directions: well- and ill-intentioned governments, eager to learn about their citizens' lives, or focused on protecting them from terrorist threats count among them, but so do commercial enterprises interested in turning personal data into revenue streams or wanting to maximize service to their customers. Whether firms like *Facebook* or *Google* – whose customers number in the hundreds of millions – use their accumulated knowledge in the right way has thus become a subject of debate in recent years. Most discussion about threats to privacy today has to do with the connectedness and linkage of personal or person-related data through the Internet. Both public and private sector actors have responded to these worries with attempts at (self-)regulation, on the national and on the international level. However, much of this field remains contested and little has been achieved in terms of encompassing goals and standards for such regulation. Since June 2013, privacy has also come on the political agenda in many countries after revelations about systematic snooping by security agencies such as the National Security Agency (NSA) in the United States, Government Communications Headquarters (GCHQ) in the United Kingdom, and Bundesnachrichtendienst (BND) in Germany emerged.

Privacy and Technology

While privacy is a basic human need and is constitutive for the individual, it remains difficult to describe and define. Across societies, the desire and need for privacy has varied historically (Moore, 1984), and in the process of modernization, demand for privacy has tended to grow in order to balance societal intrusions resulting from developments such as greater population density. In the theoretical debate, however, no generally accepted definition has so far emerged. More than 45 years ago, Alan Westin (1967, p. 7) wrote in his seminal study on the subject: "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists." A recent comprehensive work in the area makes basically the same point when it states: "Privacy, however, is a concept in disarray. Nobody can articulate what it means." (Solove, 2008, p. 1). The main reason for this lies in the fact that privacy is defined negatively as an absence of intrusion; such intrusions, however, can come from many directions and vary in type and subjectively perceived intensity, hence leading to different priorities for their avoidance.

Discussions about privacy and its intrusions have almost always been linked to technological developments. Already in the late nineteenth century, the emergence of 'instantaneous photographs' was seen as invading privacy, prompting calls for a right "to be let alone" (Warren/Brandeis, 1890). In the 1920s, the tapping of telephone lines for purposes of law enforcement led to debates resulting in stringent regulation and reporting requirements for such actions. In the 1960s and 1970s, plans for comprehensive 'data banks' and 'national data centers' containing electronic records of every citizen prompted debates about the relative merits of optimizing the state's social planning versus protecting privacy (Miller, 1971) and stopped most of these developments. From the 1990s onward, the proliferation of CCTV systems led to discussions about a 'surveillance society,' in which there was "no place to hide" (O'Harrow, 2006), as every move could be watched and recorded. After the terrorist attacks in the United States on 11 September 2001, plans emerged to put technology to the service of antiterrorism, but technocratic dreams of 'Total Information Awareness' through 'data mining' of all available public and private sector information sources turned out to be neither feasible nor desirable (National Research Council, 2008).

In the context of technology, privacy almost always means informational privacy and thus focuses on a specific part of the debate about privacy (Rössler, 2005). Analyzing the relationship between the Internet and privacy thus requires looking at the competing interests over person-related data as well as at the

http://dx.doi.org/10.1016/B978-0-08-097086-8.75024-0

International Encyclopedia of the Social & Behavioral Sciences, Second Edition, 2015, 593–599

attempts to set rules about their creation, proliferation, storage, and use.

Internet Use and Personal Data

Development of Internet Usage

Usage of the Internet has made the transition from expert domain to everyday use in the last two decades. Originally developed by military and academic experts to provide a safe means of communications even in the event of a nuclear war, and used first to link up leading research centers, the 'Internet' is actually a system of various connected computer networks that function by adhering to common technical protocols. Hiding the underlying complexity from the user and making a vast network of billions of nodes easily maneuverable through naming systems and graphical interfaces has been a condition for its exploding usage as well as for its commercial success, with the latter providing the funds for the Internet's ever-increasing capacity.

Internet use has increased dramatically since the turn of the century. In 2000, the percentage of individuals using the Internet was between 20% and 40% in developed countries (France: 14%; UK: 27%; Germany and Japan: 30%; US: 43%), and the global number was at a mere 6.5%. By 2013, numbers had shot up to around 85% in the first group (US: 84%; France: 82%; Japan: 86%; UK: 90%; Germany: 84%), while the global number had increased sixfold to 40% ('ITU database' http://www.itu.int/). This massive growth was unexpected even by experts who did not foresee the explosive development of mobile Internet access at broadband speeds which helped in particular to connect citizens of developing countries to the Internet in only a few years. As a result, an estimated 2.7 billion people around the globe had access to and used the Internet in 2013 (International Telecommunication Union, 2013, p. 1).

While these impressive growth figures have contributed substantially to development goals in developing countries (where they have, e.g., helped to introduce mobile banking and to spread public health and education information), it is in the developed countries that commercial activity initiated by and through the Internet is strongest. Electronic commerce has been a growth engine in many developed economies, contributing further to a shift toward a knowledge and information-based economy that has been under way at least since the 1960s (Machlup, 1962). But the Internet has also triggered the emergence and meteoric rise of new corporate stars such as Google (search engine) and Facebook (social media). These firms (which are used here as illustration for many others that are similar) build their business models on the use and processing of person-related data, for they charge no fees for their services from their customers. Instead, customers pay indirectly with their personal data which firms – through sophisticated mechanisms – monitor, store, and then use to create profiles. These profiles in turn allow them to sell advertisements which are highly targeted to the user's sociodemographic characteristics, thus increasing their success rate and extracting premium prices from advertisers.

How much successful firms like Google and Facebook depend on this business model is evident from business data submitted in companies' quarterly reports to the US Securities and Exchange Commission (SEC): in the first half of 2012, advertising revenues made up 96% of Google's overall revenues; and Facebook (which reported 955 million 'monthly active users' and 552 million 'daily active users') earned 84% of its total revenue from advertising ('SEC,' http://www.sec.gov/). In short, these firms would not be commercially viable without advertising revenues from personal data.

User Demand for Internet Privacy

In their corporate mission statements firms like Google and Facebook neither mention the commercial use they make of person-related data nor their dependency on them. They describe their mission as, respectively, "to organize the world's information and make it universally accessible and useful" (Google) and "to make the world more open and connected" (Facebook).

Being more open about their actual business models might cause worries among the hundreds of millions of customers who use their services on a daily basis. Google, for example, answers between four and five billion search questions per day; it logs and keeps all search queries as well as users' IP addresses, in addition to 'cookies' (small data files that track a user's Web browsing), and (where applicable) location information ('Google,' https://www.google.com/policies/privacy/). Thus the firm obtains a lot of person-related data which it may combine with information that users turn over voluntarily when registering for a user account with the firm, such as name, e-mail address as well as telephone and credit card numbers or device identifiers. Given that the company's market share is 95% of the search engine market in some European countries, this means that users may have few alternatives to using these services.

According to surveys, users value their privacy highly and are concerned about the protection of their personal data on the Internet. General worries about privacy and data protection predate the advent of the Internet, but the availability of online electronic commerce means most consumers were only confronted concretely with the issue of being asked to enter personal data online in the late 1990s. In an internationally comparative survey commissioned by IBM, 80% of respondents in the US, 68% in the UK, and 79% in Germany agreed with the statement "Consumers have lost all control over how personal information is collected and used by companies" (Louis Harris & Associates, 1999, p. 22). Data from the Eurobarometer survey show that the level of 'concern' about data privacy has changed little since the early 1990s, with 68% expressing it in 2008 and 66% in 1991 – the worries are thus not primarily triggered by the Internet. Underlying this stable trend, however, are substantial differences in attitudes between countries: Austria and Germany top the field with a rising trend and 86% expressing concern, while at the bottom of the list are Finland and the Netherlands with 35% and 32% respectively and (in the latter case) a declining trend. With respect to the Internet specifically, worries tend to be more pronounced: 82% of EU respondents thought that data transmission over the Internet was not sufficiently secure, with some variation across countries but little across sociodemographic differences (Gallup Europe/European Commission, 2008). On the other hand, the disclosure of personal information is seen by many as a part of modern life. They do disclose such information for the purposes of online services and online shopping, but 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than for which it was collected (European Commission/TNS Opinion and Social, 2011).

In sum, a strong preference for privacy, and worries about safety of personal data submitted online do not prevent citizens from using the Internet for online activity, but survey evidence indicates that they use it in a guarded way.

Problems of Crime, Security, and Surveillance on the Internet

The Internet was originally designed without central control in order to maximize the autonomy of heterogeneous networks working together. This not only conformed with military priorities of resilience in the case of a nuclear attack, it was also appropriate for the relatively small academic community in which users trusted each other; in addition it resonated with the libertarian impulses of the founding generation of engineers many of whom had links to the counterculture (Markoff, 2006). The result has been interpreted as a 'techno-utopian' attempt at self-regulation (Hofmann, 2012), a space almost completely free from formal boundaries and rules, in which the eventual emergence of problems with cybercrime is primarily an unforeseen consequence of past design decisions.

Cybercrime and Cybersecurity

What is now labeled 'cybercrime' has been emerging from the mid-1990s onward – when the originally wholly state-funded backbones were privatized and commercial use of the Internet took off – and taken various forms. The sending of unsolicited mass messages to initially many thousands, later millions of users advertising goods and services ('spam') was a first (and more annoying than dangerous) way of using the Internet for unintended activities. Initially done through e-mail (making use of the open nature of Internet e-mail servers), this activity was more recently primarily conducted through 'botnets' of PCs that had been taken over through the installation of malware. Such malware (viruses and 'trojans') can also be used to obtain passwords by logging and sending out users' keystrokes or to scan hard drives for files containing confidential information. Individual servers on the Internet, but also whole networks of firms or governments can be attacked through flooding them with IP packets (often from botnets), thus effectively shutting them down ('distributed denial of service'); and such attacks can be combined with attempts at extortion. Other forms of cybercrime include the sending of e-mail which claims to be from a user's bank or business partner, but which contain links redirecting responses to forged Web sites ('phishing') and the systematic use of personal data to impersonate other people for fraudulent purposes ('identity theft').

It is very difficult to obtain reliable information about the scale of the problem of cybercrime. Figures about its costs often make headlines – the British *Financial Services Authority*, e.g., estimated the cost of identity fraud to the UK economy at £1.7 billion per annum. This estimate, however, includes substantial amounts for lost or stolen credit cards, VAT losses, and even costs to state agencies for antifraud procedures. Furthermore, crime statistics do not routinely count whether IT was instrumental in committing a crime. Without more precisely targeted attempts to identify crimes committed online, a UK public inquiry concluded, "it is simply impossible to assess the scale of the problem" (House of Lords. Select Committee on the Constitution, 2009, vol. 1, pp. 15–16). As regards the inflated headline figures, it is clear that both in the public sector (law enforcement) and in the private sector (IT security firms) some actors clearly have an interest in pushing publicity of the issue.

Internet users, as far as survey evidence shows, have taken the dangers to heart and modified their behavior accordingly by trying to protect their privacy. 40% of Internet users in the EU are concerned about someone stealing or misusing their personal data; and 38% worry about the security of their online payments. Many of them have therefore changed their online behavior, and most of them try to avoid disclosing personal information online. When using the Internet for online banking or shopping, the two most common concerns are about someone taking or misusing personal data (mentioned by 40% of Internet users in the EU) and security of online payments (38%) (European Commission/TNS Opinion & Social, 2012, p. 4).

Both private and public sector actors have reacted to the threat and to the worries of users. IT security firms developed sophisticated tools to protect their customers' PCs from attacks through viruses and other malware and have built a substantial business around this; states have initiated international agreements (like the 2001 *Convention on Cybercrime* by the Council of Europe which contains common definitions and procedures on the subject as well as rules for international cooperation), passed national legislation, and set up competence centers to develop appropriate defenses.

Surveillance on the Internet

Security firms and state agencies thus work to protect users' privacy against illegitimate and foreign intrusion. But in order to do that, they collect lots of personal data which means we can look at the very same actors also with reference to the debate about surveillance. That debate focuses on how users on the Internet can be protected from the actions of legitimate firms and government agencies, and has been the subject of considerable social activism (Bennett, 2008). Firms' commercial interests were already mentioned above; government agencies, in turn, have an interest in using the Internet for the collection of person-related data for purposes of state and policy administration, social planning, law enforcement, national security, etc.

The concept of surveillance has been prominent in the sociological literature on personal and person-related information in recent years and has given rise to the academic field of *surveillance studies* (for an overview see Lyon, 2007; Ball et al., 2012). In this debate, the term surveillance has been defined very broadly as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon, 2007, p. 14), and as a consequence, much has been described and discussed in this literature. Most of this is not or only indirectly linked to the Internet, such as CCTV cameras in public space, workplace surveillance practices of employers, DNA databases for policing or the tagging of consumption patterns through radio frequency identification chips or 'smart meters.' With the growing use and commercialization of the Internet from the mid-1990s onward, surveillance has also taken place through the Internet (e.g., through easy availability of background checks, and the massive collection of data to monitor and profile Internet users). Increasing transparency of individuals' actions is the result of these developments – often without their awareness. However, literature from the *surveillance studies* tradition has been criticized for being somewhat one-sided and pessimistic in its assessment of surveillance on the Internet and furthermore poor on empirical and technical detail (Bennett/Parsons, 2013).

While surveillance from the private sector is (at least in principle) subject to attempts at regulation on the national and supranational level, even if their extent is contested (see below), this is much less the case for surveillance from the public sector. As studies conducted by the OpenNet Initiative have demonstrated, Internet censorship and surveillance are becoming more technically sophisticated, and both are increasingly prevalent not only in authoritarian regimes, but also in liberal democracies (Deibert et al., 2010). As a result, the initially almost universally optimistic assessment of the emancipatory societal and political consequences of further spread of Internet use – prominently visible, e.g., in the role played by social media during the 'Arab Spring' of 2011 – has been called into question. Rather than bringing empowerment to the individual, fostering transparency and democracy, and undermining authoritarian rule, it has been pointed out, the surveillance potential of Internet technology can also be used by dictatorships to spy on dissidents, uncover their identities, and censor access to information (Morozov, 2011). The revelations of routine and widespread snooping by national security agencies that surfaced in the summer of 2013 and are discussed in a separate section below have contributed to increased sensitivity in this area in many countries.

Regulating Privacy on the Internet

Problems to protect privacy against intrusions are in principle amenable to solutions through regulation. Like in most other policy domains, attempts to impose such regulations meet resistance from interested parties and political forces opposed to regulation. But there are two domain-specific aspects that further complicate regulation of privacy on the Internet: on the one hand, due to its purposefully decentralized technical nature, there is not one single point from which the whole of the Internet can be affected by regulation; and on the other hand, attempts at regulation only started after the privatization of the Internet backbones and the opening up of the Internet for commercial use, i.e., in the mid-1990s. At that point in time, however, the Internet had already undergone a long period without any regulation, while privacy regulation had been under way for some time, both on the national and international level, without taking into account the specific problems the Internet created in that area. Attempts at regulation thus continue to take place in a highly fragmented situation, with a multitude of actors (many of whom focus not only on regulation on the Internet) and strongly diverging interests. Outcomes are therefore often characterized by conflict and blockade.

National Level Regulation

Due to the technical aspects of the Internet and the sequence of historical developments mentioned above, regulation of privacy on the national level is not primarily focused on the Internet. Privacy became a topic of political regulation in many Western democracies in the 1970s, when countries (starting with Sweden and West Germany) began to discuss and pass comprehensive privacy legislation and set up institutions charged with protecting personal information, often labeled 'privacy commissioners' or 'data protection agencies.' While reacting to common problems, national solutions varied considerably due to varying political preferences, administrative traditions, and institutional interests; but processes of diffusion and learning spread privacy legislation across the globe in the decades since (Newman, 2008). The United States, however, followed a different trajectory with a focus on performance-based regulation centering on 'fair information principles' largely developed by the administration, and supplemented by area-specific legislation instead of comprehensive legislation.

National regulators and privacy commissioners have little effective influence on the whole Internet. Their work thus mainly focuses on national level implementation of rules and questions that are amenable to national regulation. Under the heading 'Internet,' a recent report (published in 2011) of the German Data Protection Commissioner, e.g., discussed such topics as the collection of location data, WLAN access, Google Street View, and the setting up of a 'Common Internet Center' by German security authorities to fight terrorism. Such reports can influence national political debates, serve as an antagonist to security agency and law enforcement interests in the political process, and have educational effects on the general public which uses the Internet, but it is unlikely to achieve much beyond national borders. Borrowing a term from environmental policy, it can thus primarily be described as 'end-of-pipe regulation.'

International Level Regulation

Potentially more effective regulation can be achieved on the supranational and international level. Indeed, looking at privacy regulation, one can say that the international level has been leading the way here, with bodies such as the Council of Europe and the OECD being early initiators of conventions and guidelines from the 1970s onward. In 1985, the OECD first adopted a 'Declaration on Transborder Data Flows' which pledged support for international exchange of data and information and (given its focus on economic policy) framed obstacles to it as protectionist; in 1998, a 'Declaration on the Protection of Privacy on Global Networks' followed which confirmed the importance of effective privacy protection also for the future success of e-commerce. In 1995, the European Union passed its 'Directive on the Protection of Personal Data' in order to harmonize regulation across its then 15 member states and restrict the transfer of personal data to third countries without adequate protection of personal data. Since EU directives are legally binding to member states, this had more direct impact than the previous documents which largely had the status of recommendations.

However, none of these supranational and international organizations are in a position to exercise direct regulatory power over the Internet. Indeed, who controls the Internet is both unclear and contested (Goldsmith/Wu, 2006); and given the principal decisions in favor of technological openness that lie at the heart of the Internet (see above), the fact that a single set of standards cannot be enforced universally on the whole Internet will not change. Furthermore, conceptions and priorities regarding privacy vary on the national level: European countries perceive privacy as a fundamental human right which is a precondition for an individual's autonomy; it can therefore not be given up individually, and society has a duty to protect it. In the United States, in contrast, privacy is seen as a property right that an individual can trade away if he or she chooses to, and markets are thus seen as a more effective way of protecting it than state regulation (Busch, 2011).

With divergent preferences between Europe and the US, no international regime governing privacy on the Internet could be established; instead, rival standards are the most likely outcome in such a situation, and that has indeed been the case (Drezner, 2007). As a consequence, conflicts have arisen over data protection on the Internet between the EU and the US in the past. While a compromise could be reached in the economically important area of e-commerce with the 'Safe Harbor Agreement' of 2000, outcomes have been more conflictuous and characterized by unilateral imposition of US preferences in areas related to security and antiterrorism policy, such as the questions of transferring personal data of aviation passengers (PNR) or international financial transactions data (SWIFT) (Busch, 2013).

The Internet and National Security

Information technology has been playing an ever more important role in security policy over the last decades due to the massive improvements in information and communications technology (ICT). This development was further speeded up significantly after the terrorist attacks of 11 September 2001, leading to a transformation of state activities which saw a blurring of the boundaries between foreign and domestic security policy, the blending of police, secret service, and military tasks, and a central role for ICT as a national security state tool (Busch, 2015).

The extent to which national security agencies have interfered with communication on the Internet in order to obtain information became clear after a whistleblower, the former NSA contractor Edward Snowden, published classified information from the summer of 2013 onward. It revealed comprehensive operations by intelligence agencies such as the US NSA, the UK's GCHQ, the German BND, and various others more to intercept information from the Internet and the telephone system through both indiscriminate bulk data collection as well as targeted spying under programs with names like PRISM, Quantum, Tempora, XKeyscore, or MUSCULAR. The material also made public a previously unknown level of cooperation and data sharing between these agencies which could also serve to circumvent constitutional barriers to their operations, such as a ban on spying against their own country's citizens. Apparently the NSA also had direct access to the servers of technology firms like Google, Facebook, Microsoft, and Apple (Harding, 2014).

The revelations ruffled feathers diplomatically as it became clear that the US had not only collected data from close allies such as Germany and France and bugged a fax machine of the European Commission, but had even targeted Chancellor Merkel's personal cell phone. As these transgressions were criticized in political discourse, they made clear that a number of state security agencies seemed to have overstepped their brief. A principal-agent problem had evidently emerged in the oversight of security services, and legislatures in some countries moved to tighten the reins. In the United States, for example, President Obama appointed a *Review Group on Intelligence and Communications Technologies* that reported in December 2013. Besides its 46 concrete recommendations the report emphasizes the need to "protect, at once, two different forms of security: national security and personal privacy" (President's Review Group, 2014, p. xv). It remains to be seen to what extent the Review Group's recommendations will result in changes to US policy. In any case a continuation of past practices could severely harm US business interests if customers from other countries decided not to entrust their electronic data to servers located in the US any longer.

Internet and Privacy: Outlook

Growing use of the Internet is only the latest in a string of technological developments that has imperiled personal privacy. While opinion polls show a strong preference of Internet users to protect their personal data, a number of interests combine to make use of such data, mainly for the purposes of economic growth, commercial profit, and the protection of individual and national security. While in principle regulation could help strike a balance between these competing interests, various factors have been working against this. Thus regulation of the Internet is principally difficult due to its decentralized nature on the technical level, its global connectedness and spread across many jurisdictions, and private ownership of large parts of its infrastructure. In addition, the view that states could not regulate the Internet (and that states are generally on the way out as globalization spreads) dominated for a long time, resulting in few attempts at regulation. When – parallel to the growing importance of the Internet – state attempts at regulation increased, they encountered collective action problems emanating from different preferences and regulatory path dependencies.

Whether competition between rival regulatory standards on the international level, mainly those of the US and the EU, will lead to the emergence of common solutions remains to be seen. While such regulation can affect privacy interests of Internet users, the resistance against that may in the future be less stringent than it was in the past, for attitudes in this area have changed, as a leading advocate in that field has stated: "When I first wrote the book, two ideas seemed to dominate debate about the Net: first, that the government could never regulate the Net, and second, that this was a good thing. Today, attitudes are different. There is still the commonplace that government can't regulate, but in a world drowning in spam, computer viruses, identity theft, copyright 'piracy', and the sexual exploitation of children, the resolve against regulation has weakened. We all love the Net. But if some government could really deliver on the promise to erase all the bads of this space, most of us would gladly sign up" (Lessig, 2006, p. 27).

In principle, a third approach to the problem of protecting privacy on the Internet – besides national and international level regulation – is available, namely a technical and organizational solution applied at the level of the information system ('privacy by design,' 'privacy enhancing technologies'). While this has both been discussed and encouraged (e.g., by information commissioners) for some time, implementation has been reluctant as substantial interests exist that push, e.g., against data minimization. Whether that balance of interests will shift as the number of Internet users rises further and discussions about the "virtue of forgetting in the digital age" (Mayer-Schönberger, 2009) become more prominent, remains open to speculation. The debate following the European Court of Justice ruling of April 2014 about the "right to be forgotten" (C131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*) has demonstrated the difficulty of balancing central values such as free speech and the protection of privacy. But above all it has been known for some time that who prevails in collective action is not primarily determined by the sheer number of people involved on both sides or the quality of the argument, but rather by their relative incentives and capabilities to organize and gain influence on the political decision-making process (Olson, 1965).

Botnet	A group of computers that are connected to the Internet and under the control of a malicious party, typically after malware (such as a virus program) has been executed under legitimate use.
Data mining	A process of attempting to discover meaningful patterns in (often very large) sets of already collected data without prior forming of hypotheses.
Privacy enhancing technologies (PET)	Technological, procedural, or organizational tools to enhance user control over their personal data.
Radio frequency identification (RFID)	A wireless technology that uses electromagnetic fields to transfer data, mostly without battery, from a tag attached to an object to identify its properties.
Total information awareness (TIA)	Program run by the US Department of Defense after 11 September 2001 to integrate information from diverse sources. After allegations of privacy violations funding was withdrawn in 2004.
Ubiquitous computing	A paradigm of computer use in which many, often mobile and networked computers replace the one traditional desktop computer

See also: Cyber Crime: Identity Theft; Cyberbullying; Internet and Culture; Internet and Social Media: Anthropological Aspects; Oversharing: The Eclipse of Privacy in the Internet Age; Privacy: Theoretical and Legal Issues; Surveillance Studies; Surveillance and Privacy, Geography of.

Bibliography

Ball, Kirstie, Haggerty, Kevin, Lyon, David (Eds.), 2012. Routledge Handbook of Surveillance Studies. Routledge, London.

Bennett, Colin J., 2008. The Privacy Advocates. Resisting the Spread of Surveillance. MIT Press, Cambridge MA.

Bennett, Colin J., Parsons, Christopher, 2013. Privacy and surveillance: the multidisciplinary literature on the capture, use, and disclosure of personal information in cyberspace. In: Dutton, William H. (Ed.), The Oxford Handbook Internet Studies. Oxford Univ. Press, Oxford, pp. 486–508.

Busch, Andreas, 2011. The regulation of privacy. In: Levi-Faur, David (Ed.), Handbook on the Politics of Regulation. Edward Elgar, Cheltenham UK, Northampton MA, pp. 227–240.

Busch, Andreas, 2013. The regulation of transborder data traffic: disputes across the Atlantic. Security and Human Rights 24, 119–138.

Busch, Andreas, 2015. The changing architecture of the National Security State. In: Leibfried, Stephan, Huber, Evelyne, Lange, Matthew, Levy, Jonah, D., Nullmeier, Frank, Stephens, John (Eds.), The Oxford Handbook of Transformations of the State. Oxford University Press, Oxford, pp. 536–553.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal, Zittrain, Jonathan (Eds.), 2010. Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press, Cambridge Mass.

Drezner, Daniel W., 2007. All Politics Is Global. Explaining International Regulatory Regimes. Princeton Univ. Press, Princeton.

European Commission and TNS Opinion & Social, 2011. Attitudes on Data Protection and Electronic Identity in the European Union. Special Eurobarometer 359. Brussels.

European Commission and TNS Opinion & Social, 2012. Cyber Security. Special Eurobarometer 390. Brussels.

Gallup Europe and European Commission, 2008. Data Protection in the European Union: Citizens' Perceptions. Analytical Report. Brussels.

Goldsmith, Jack L., Wu, Tim, 2006. Who Controls the Internet? Illusions of a Borderless World. Oxford University Press, Oxford.

Harding, Luke, 2014. The Snowden Files. The Inside Story of the World's Most Wanted Man. Guardian Books, London.

Hofmann, Jeanette, 2012. Et in Arcadia Ego: from Techno-Utopia to cybercrime. In: Margetts, Helen, 6, Perri, Hood, Christopher (Eds.), Paradoxes of Modernization. Unintended Consequences of Public Policy Reform. Oxford Univ. Press, Oxford, pp. 81–100.

House of Lords. Select Committee on the Constitution (Ed.), 2009. Surveillance: Citizens and the State. 2nd Report of Session 2008–09. The Stationery Office, London.

International Telecommunication Union, 2013. Measuring the Information Society 2013. International Telecommunication Union, Geneva.

Lessig, Lawrence, 2006. Code: Version 2.0. Basic Books, New York.

Louis Harris & Associates, Inc, 1999. IBM Multi-national Consumer Privacy Survey. A Comprehensive and Comparative Look at Consumers in the United States, Germany, and United Kingdom and Their Attitudes toward Privacy in Everyday Business Transactions. IBM Global Services, New York.

Lyon, David, 2007. Surveillance Studies. An Overview. Polity, Cambridge.

Machlup, Fritz, 1962. The Production and Distribution of Knowledge in the United States. Princeton Univ. Press, Princeton, NJ.

Markoff, John, 2006. What the Dormouse Said. How the Sixties Counterculture Shaped the Personal Computer Industry. Penguin, New York.

Mayer-Schönberger, Viktor, 2009. Delete. The Virtue of Forgetting in the Digital Age. Princeton Univ. Press, Princeton, NJ.

Miller, Arthur R., 1971. The Assault on Privacy. Computers, Data Banks, and Dossiers. University of Michigan Press, Ann Arbor.

Moore Jr., Barrington, 1984. Privacy. Studies in Social and Cultural History. M.E. Sharpe, Armonk, N.Y.; London.

Morozov, Evgeny, 2011. The Net Delusion. The Dark Side of Internet Freedom. Public Affairs, New York.

National Research Council (Ed.), 2008. Protecting Individual Privacy in the Struggle against Terrorists. A Framework for Program Assessment. National Academies Press, Washington DC.

Newman, Abraham L., 2008. Protectors of Privacy. Regulating Personal Data in the Global Economy. Cornell University Press, Ithaca ua.

O'Harrow, Robert, 2006. No Place to Hide. Behind the Scenes of of Our Emerging Surveillance Society. Free Press, New York, NY.

Olson, Mancur, 1965. The Logic of Collective Action. Public Goods and the Theory of Groups. Harvard University Press, Cambridge, Mass.

President's Review Group on Intelligence and Communications Technologies, 2014. The NSA Report. Liberty and Security in a Changing World. Princeton University Press, Princeton (NJ), Oxford.

Rössler, Beate, 2005. The Value of Privacy. Polity, Cambridge (UK), Malden (MA).

Solove, Daniel J., 2008. Understanding Privacy. Harvard University Press, Cambridge, Mass.

Sommer, Peter, Brown, Ian, 2011. Reducing Systemic Cybersecurity Risk. OECD/IFP Project on "Future Global Shocks". 14th January 2011. Paris.

Warren, Samuel D., Brandeis, Louis D., 1890. The right to privacy. Harvard Law Review IV, 193–220.

Westin, Alan F., 1967. Privacy and Freedom. Atheneum, New York.

Relevant Websites

https://www.google.com/policies/privacy/ – Google.
http://www.itu.int/ITU-D/ict/statistics/explorer/index.html – ITU database.
http://www.sec.gov/ – U.S. Securities and Exchange Commission.