Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps with security, which can include the concepts of appropriate use and protection of information. Privacy may also take the form of bodily integrity. The right not to be subjected to unsanctioned invasions of privacy by the government, corporations, or individuals is part of many countries' privacy laws, and in some cases, constitutions.

In the business world, a person may volunteer personal details, including for advertising, in order to receive some kinds of benefit. Public figures may be subject to rules on the public interest. Personal information which is voluntarily shared but subsequently stolen or misused can lead to identity theft.

The concept of universal individual privacy is a modern concept primarily associated with Western culture, British and North American in particular, and remained virtually unknown in some cultures until recent times. Most cultures, however, recognize the ability of individuals to withhold certain parts of their personal information from wider society, such as closing the door to one's home.

Contents

History

Privacy has historical roots in ancient Greek philosophical discussions. The most well-known of these was Aristotle's distinction between two spheres of life: the public sphere of the *polis*, associated with political life, and the private sphere of the *oikos*, associated with domestic life.[1] In the United States, more systematic treatises of privacy did not appear until the 1890s, with the development of privacy law in America.[1]

Technology

As technology has advanced, the way in which privacy is protected and violated has changed with it. In the case of some technologies, such as the printing press or the Internet, the increased ability to share information can lead to new ways in which privacy can be breached. It is generally agreed that the first publication advocating privacy in the United States was the 1890 article by Samuel Warren and Louis Brandeis, "The Right to Privacy",[2] and that it was written largely in response to the increase in newspapers and photographs made possible by printing technologies.[3]

In the 1960s, people began to consider how changes in technology were bringing changes in the concept of privacy.[4] Vance Packard's *The Naked Society* was a popular book on privacy from that era and led US discourse on privacy at that time.[4]

New technologies can also create new ways to gather private information. For example, in the United States it was thought that heat sensors intended to be used to find marijuana-growing operations would be acceptable. However, in 2001 in *Kyllo v. United States* (533 U.S. 27) it was decided that the use of thermal imaging devices that can reveal previously unknown information without a warrant does indeed constitute a violation of privacy.[5] In 2019, after developing a corporate rivalry in competing voice-recognition software, Apple and Amazon required employees to listen to intimate moments and faithfully transcribe the contents.[6]

Advertisement with a highlighted quote "my face got redder and redder!" There is a highlighted quote on the importance of being honest with oneself, and after two and a half pages concludes with a suspicion that telephone operators are listening in on every call.

Police and government

Internet

Andrew Grove, co-founder and former CEO of Intel Corporation, offered his thoughts on internet privacy in an interview published in May 2000:[7]

> Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age.

Advertisement for dial telephone service available to delegates to the 1912 Republican convention in Chicago. A major selling point of dial telephone service was that it was "secret", in that no operator was required to connect the call.

Legal discussions of Internet privacy

The Internet has brought new concerns about privacy in an age where computers can permanently store records of everything: "where every online photo, status update, Twitter post and blog entry by and about us can be stored forever", writes law professor and author Jeffrey Rosen.[8]

Social networking

Several online social network sites (OSNs) are among the top 10 most visited websites globally. Facebook for example, as of August 2015, was the largest social-networking site, with nearly 2.7 billion[9] members, who upload over 4.75 billion pieces of content daily. While Twitter is significantly smaller with 316 million registered users, the US Library of Congress recently announced that it will be acquiring and permanently storing the entire archive of public Twitter posts since 2006, reports Rosen.[8]

A review and evaluation of scholarly work regarding the current state of the value of individuals' privacy of online social networking show the following results: "first, adults seem to be more concerned about potential privacy threats than younger users; second, policy makers should be alarmed by a large part of users who underestimate risks of their information privacy on OSNs; third, in the case of using OSNs and its services, traditional one-dimensional privacy approaches fall short".[10] This is exacerbated by deanonymization research indicating that personal traits such as sexual orientation, race, religious and political views, personality, or intelligence can be inferred based on a wide variety of digital footprints, such as samples of text, browsing logs, or Facebook Likes.[11]

Intrusions of social media privacy are known to affect employment in the United States. Microsoft reports that 75 percent of U.S. recruiters and human-resource professionals now do online research about candidates, often using information provided by search engines, social-networking sites, photo/video-sharing sites, personal web sites and blogs, and Twitter. They also report that 70 percent of U.S. recruiters have rejected candidates based on internet information. This has created a need by many to control various online privacy settings in addition to controlling their online reputations, the conjunction of which has led to legal suits against both social media sites and US employers.[8]

Selfie culture

Selfies are popular today. A search for photos with the hashtag #selfie retrieves over 23 million results on Instagram and 51 million with the hashtag #me.[12] However, due to modern corporate and governmental surveillance, this may pose a risk to privacy.[13] In a research study which takes a sample size of 3763, researchers found that for users posting selfies on social media, women generally have greater concerns over privacy than men, and that users' privacy concerns inversely predict their selfie behavior and activity.[14]

Online harassment

Bot accounts

Since May 2019, Facebook has removed more than 3 billion accounts. Over 83.09 million accounts were fake.[15] More than 20 million of Twitter's users are bots.

Privacy and location-based services

Increasingly, mobile devices facilitate location tracking. This creates user privacy problems. A user's location and preferences constitute personal information. Their improper use violates that user's privacy. A recent MIT study by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity.[16]

Several methods to protect user privacy in location-based services have been proposed, including the use of anonymizing servers, blurring of information e.a. Methods to quantify privacy have also been proposed, to calculate the equilibrium between the benefit of providing accurate location information and the drawbacks of risking personal privacy.[17]

Advertising on mobile devices

In recent years, seen with the increasing importance of mobile devices and paired with the *National Do Not Call Registry*, telemarketers have turned attention to mobiles.[18] Additionally, Apple and Google are constantly improving their privacy technology. With iOS 13, Apple introduced Sign in with Apple[19] and Google introduced allowing location access only when the app is in-use.[20]

Ethical controversies over location privacy

According to some experts, many commonly used communication devices may be mapping every move of their users. US Senator Al Franken has noted the seriousness of iPhones and iPads having the ability to record and store users' locations in unencrypted files,[21] although Apple denied doing so.[22]

In 2021, the US state of Arizona found that "Google Misleads and Deceives Users Regarding Its Deletion of Their Location", among other allegations.[23]

Metadata

The ability to do online inquiries about individuals has expanded dramatically over the last decade. Importantly, directly observed behaviour, such as browsing logs, search queries, or contents of a public Facebook profile, can be automatically processed to infer secondary information about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality.[24]

In Australia, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 made a distinction between collecting the contents of messages sent between users and the metadata surrounding those messages.

Protection of privacy on the Internet

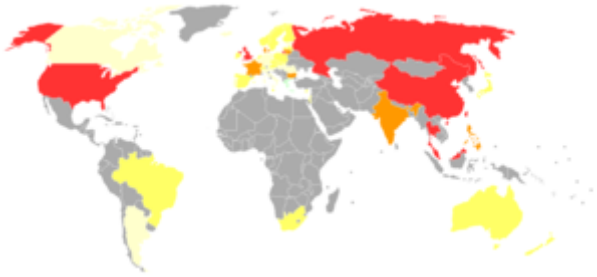
Covert collection of personally identifiable information has been identified as a primary concern by the U.S. Federal Trade Commission.[25] Although some privacy advocates recommend the deletion of original and third-party HTTP cookies, Anthony Miyazaki, marketing professor at Florida International University and privacy scholar, warns that the "elimination of third-party cookie use by Web sites can be circumvented by cooperative strategies with third parties in which information is transferred after the Web site's use of original domain cookies."[26] As of December 2010, the Federal Trade Commission is reviewing policy regarding this issue as it relates to behavioral advertising.[25]

Legal right to privacy

Most countries give citizens rights to privacy in their constitutions.[4] Representative examples of this include the Constitution of Brazil, which says "the privacy, private life, honor and image of people are inviolable"; the Constitution of South Africa says that "everyone has a right to privacy"; and the Constitution of the Republic of Korea says "the privacy of no citizen shall be infringed.[4]" The Italian Constitution also defines the right to

privacy.[27] Among most countries whose constitutions do not explicitly describe privacy rights, court decisions have interpreted their constitutions to intend to give privacy rights.[4]

Many countries have broad privacy laws outside their constitutions, including Australia's Privacy Act 1988, Argentina's Law for the Protection of Personal Data of 2000, Canada's 2000 Personal Information Protection and Electronic Documents Act, and Japan's 2003 Personal Information Protection Law.[4]



Privacy International 2007 privacy ranking
green: Protections and safeguards
red: Endemic surveillance societies

Beyond national privacy laws, there are international privacy agreements.[28] The United Nations Universal Declaration of Human Rights says "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation."[4] The Organisation for Economic Co-operation and Development published its Privacy Guidelines in 1980. The European Union's 1995 Data Protection Directive guides privacy protection in Europe.[4] The 2004 Privacy Framework by the Asia-Pacific Economic Cooperation is a privacy protection agreement for the members of that organization.[4]

Argument against legal protection of privacy

In recent years there have been only few in comparison to what? attempts to clearly and precisely define a "right to privacy." Some experts assert that in fact the right to privacy "should not be defined as a separate legal right" at all. By their reasoning, existing laws relating to privacy in general should be sufficient.[29] It has therefore proposed a working definition for a "right to privacy":

> *The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.*[29]

Free market vs consumer protection

Approaches to privacy can, broadly, be divided into two categories: free market or consumer protection.[30]

One example of the free market approach is to be found in the voluntary OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[31] The principles reflected in the guidelines are analysed in an article putting them into perspective with concepts of the GDPR put into law later in the European Union.[32]

In a consumer protection approach, in contrast, it is claimed that individuals may not have the time or knowledge to make informed choices, or may not have reasonable alternatives available. In support of this view, Jensen and Potts showed that most privacy policies are above the reading level of the average person.[33]

By country

Australia

The *Privacy Act 1988* is administered by the Office of the Australian Information Commissioner. Privacy law has been evolving in Australia for a number of years. The initial introduction of privacy law in 1998 extended to the public sector, specifically to Federal government departments, under the Information Privacy Principles. State government agencies can also be subject to state based privacy legislation. This built upon the already existing privacy requirements that applied to telecommunications providers (under Part 13 of the *Telecommunications Act 1997*), and confidentiality requirements that already applied to banking, legal and patient / doctor relationships.[34]

In 2008 the Australian Law Reform Commission (ALRC) conducted a review of Australian privacy law and produced a report titled "For Your Information".[35] Recommendations were taken up and implemented by the Australian Government via the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.[36]

In 2015, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 was passed, to some controversy over its human rights implications and the role of media.

European Union

Although there are comprehensive regulations for data protection in the European Union, one study finds that despite the laws, there is a lack of enforcement in that no institution feels responsible to control the parties involved and enforce their laws.[37] The European Union also champions the Right to be Forgotten concept in support of its adoption by other countries.[38]

India

Due to the introduction of the Aadhaar project, inhabitants of India were afraid that their privacy could be invaded. The project was also met with mistrust regarding the safety of the social protection infrastructures.[39] To tackle the fear amongst the people, India's supreme court put a new ruling into action that stated that privacy from then on was seen as a fundamental right.[40]

United Kingdom

In the United Kingdom, it is not possible to bring an action for invasion of privacy. An action may be brought under another tort (usually breach of confidence) and privacy must then be considered under EC law. In the UK, it is sometimes a defence that disclosure of private information was in the public interest.[41] There is, however, the Information Commissioner's Office (ICO), an independent public body set up to promote access to official information and protect personal information. They do this by promoting good practice, ruling on eligible complaints, giving information to individuals and organisations, and taking action when the law is broken. The relevant UK laws include: Data Protection Act 1998; Freedom of Information Act 2000; Environmental Information Regulations 2004; Privacy and Electronic Communications Regulations 2003. The ICO has also provided a "Personal Information Toolkit" online which explains in more detail the various ways of protecting privacy online.[42]

United States

Although the US Constitution does not explicitly include the right to privacy, individual as well as locational privacy are implicitly granted by the Constitution under the 4th Amendment.[43] The Supreme Court of the United States has found that other guarantees have "penumbras" that implicitly grant a right to privacy against government intrusion, for example in *Griswold v. Connecticut* (1965). In the United States, the right of freedom of speech granted in the First Amendment has limited the effects of lawsuits for breach of privacy. Privacy is regulated in the US by the Privacy Act of 1974, and various state laws. The Privacy Act of 1974

only applies to Federal agencies in the executive branch of the Federal government.[44] Certain privacy rights have been established in the United States via legislation such as the Children's Online Privacy Protection Act (COPPA),[45] the Gramm–Leach–Bliley Act (GLB), and the Health Insurance Portability and Accountability Act (HIPAA). [46]

Unlike the EU and most EU-member states, the US does not recognize the right to privacy to others than US citizens. The UN's Special Rapporteur on the right to privacy, Joseph A. Cannataci, criticized this distinction.[47]

Conceptions of privacy

Right to be let alone

In 1890, the United States jurists Samuel D. Warren and Louis Brandeis wrote "The Right to Privacy", an article in which they argued for the "right to be let alone", using that phrase as a definition of privacy.[48] This concept relies on the theory of natural rights and focuses on protecting individuals. The citation was a response to recent technological developments, such as photography, and sensationalist journalism, also known as yellow journalism.[49]

There is extensive commentary over the meaning of being "let alone", and among other ways, it has been interpreted to mean the right of a person to choose seclusion from the attention of others if they wish to do so, and the right to be immune from scrutiny or being observed in private settings, such as one's own home.[48] Although this early vague legal concept did not describe privacy in a way that made it easy to design broad legal protections of privacy, it strengthened the notion of privacy rights for individuals and began a legacy of discussion on those rights in the US.[48]

Limited access

Limited access refers to a person's ability to participate in society without having other individuals and organizations collect information about them.[50]

Various theorists have imagined privacy as a system for limiting access to one's personal information.[50] Edwin Lawrence Godkin wrote in the late 19th century that "nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion."[50][51] Adopting an approach similar to the one presented by Ruth Gavison[52] Nine years earlier,[53] Sissela Bok said that privacy is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention."[50][54]

Control over information

Control over one's personal information is the concept that "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Generally, a person who has consensually formed an interpersonal relationship with another person is not considered "protected" by privacy rights with respect to the person they are in the relationship with. [55][56] Charles Fried said that "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves. Nevertheless, in the era of big data, control over information is under pressure.[57]

States of privacy

Alan Westin defined four states—or experiences—of privacy: solitude, intimacy, anonymity, and reserve. Solitude is a physical separation from others;[58] Intimacy is a "close, relaxed; and frank relationship between two or more individuals" that results from the seclusion of a pair or small group of individuals.[58] Anonymity is the "desire of individuals for times of 'public privacy.'"[58] Lastly, reserve is the "creation of a psychological barrier against unwanted intrusion"; this creation of a psychological barrier requires others to respect an individual's need or desire to restrict communication of information concerning himself or herself.[58]

In addition to the psychological barrier of reserve, Kirsty Hughes identified three more kinds of privacy barriers: physical, behavioral, and normative. Physical barriers, such as walls and doors, prevent others from accessing and experiencing the individual.[59] (In this sense, "accessing" an individual includes accessing personal information about him or her.)[59] Behavioral barriers communicate to others—verbally, through language, or non-verbally, through personal space, body language, or clothing—that an individual does not want them to access or experience him or her.[59] Lastly, normative barriers, such as laws and social norms, restrain others from attempting to access or experience an individual.[59]

Secrecy

Privacy is sometimes defined as an option to have secrecy. Richard Posner said that privacy is the right of people to "conceal information about themselves that others might use to their disadvantage". [60][61]

In various legal contexts, when privacy is described as secrecy, a conclusion if privacy is secrecy then rights to privacy do not apply for any information which is already publicly disclosed.[62] When privacy-as-secrecy is discussed, it is usually imagined to be a selective kind of secrecy in which individuals keep some information secret and private while they choose to make other information public and not private.[62]

Personhood and autonomy

Privacy may be understood as a necessary precondition for the development and preservation of personhood. Jeffrey Reiman defined privacy in terms of a recognition of one's ownership of his or her physical and mental reality and a moral right to his or her self-determination.[63] Through the "social ritual" of privacy, or the social practice of respecting an individual's privacy barriers, the social group communicates to the developing child that he or she has exclusive moral rights to his or her body—in other words, he or she has moral ownership of his or her body.[63] This entails control over both active (physical) and cognitive appropriation, the former being control over one's movements and actions and the latter being control over who can experience one's physical existence and when.[63]

Alternatively, Stanley Benn defined privacy in terms of a recognition of oneself as a subject with agency—as an individual with the capacity to choose.[64] Privacy is required to exercise choice.[64] Overt observation makes the individual aware of himself or herself as an object with a "determinate character" and "limited probabilities."[64] Covert observation, on the other hand, changes the conditions in which the individual is exercising choice without his or her knowledge and consent.[64]

In addition, privacy may be viewed as a state that enables autonomy, a concept closely connected to that of personhood. According to Joseph Kufer, an autonomous self-concept entails a conception of oneself as a "purposeful, self-determining, responsible agent" and an awareness of one's capacity to control the boundary between self and other—that is, to control who can access and experience him or her and to what extent.[65] Furthermore, others must acknowledge and respect the self's boundaries—in other words, they must respect the individual's privacy.[65]

The studies of psychologists such as Jean Piaget and Victor Tausk show that, as children learn that they can control who can access and experience them and to what extent, they develop an autonomous self-concept.[65] In addition, studies of adults in particular institutions, such as Erving Goffman's study of "total institutions" such as prisons and mental institutions,[66] suggest that systemic and routinized deprivations or violations of privacy deteriorate one's sense of autonomy over time.[65]

Self-identity and personal growth

Privacy may be understood as a prerequisite for the development of a sense of self-identity. Privacy barriers, in particular, are instrumental in this process. According to Irwin Altman, such barriers "define and limit the boundaries of the self" and thus "serve to help define [the self]."[67] This control primarily entails the ability to regulate contact with others.[67] Control over the "permeability" of the self's boundaries enables one to control what constitutes the self and thus to define what is the self.[67]

In addition, privacy may be seen as a state that fosters personal growth, a process integral to the development of self-identity. Hyman Gross suggested that, without privacy—solitude, anonymity, and temporary releases from social roles—individuals would be unable to freely express themselves and to engage in self-discovery and self-criticism.[65] Such self-discovery and self-criticism contributes to one's understanding of oneself and shapes one's sense of identity.[65]

Intimacy

In a way analogous to how the personhood theory imagines privacy as some essential part of being an individual, the intimacy theory imagines privacy to be an essential part of the way that humans have strengthened or intimate relationships with other humans.[68] Because part of human relationships includes individuals volunteering to self-disclose most if not all personal information, this is one area in which privacy does not apply.[68]

James Rachels advanced this notion by writing that privacy matters because "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people."[68][69] Protecting intimacy is at the core of the concept of sexual privacy, which law professor Danielle Citron argues should be protected as a unique form of privacy.[70]

Physical privacy

Physical privacy could be defined as preventing "intrusions into one's physical space or solitude."[71] An example of the legal basis for the right to physical privacy is the U.S. Fourth Amendment, which guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures".[72]

Physical privacy may be a matter of cultural sensitivity, personal dignity, and/or shyness. There may also be concerns about safety, if, for example one is wary of becoming the victim of crime or stalking.[73]

Organizational

Government agencies, corporations, groups/societies and other organizations may desire to keep their activities or secrets from being revealed to other organizations or individuals, adopting various security practices and controls in order to keep private information confidential. Organizations may seek legal protection for their

secrets. For example, a government administration may be able to invoke executive privilege[74] or declare certain information to be classified, or a corporation might attempt to protect valuable proprietary information as trade secrets.[72]

Privacy self-synchronization

Privacy self-synchronization is a hypothesized mode by which the stakeholders of an enterprise privacy program spontaneously contribute collaboratively to the program's maximum success. The stakeholders may be customers, employees, managers, executives, suppliers, partners or investors. When self-synchronization is reached, the model states that the personal interests of individuals toward their privacy is in balance with the business interests of enterprises who collect and use the personal information of those individuals.[75]

An individual right

David Flaherty believes networked computer databases pose threats to privacy. He develops 'data protection' as an aspect of privacy, which involves "the collection, use, and dissemination of personal information". This concept forms the foundation for fair information practices used by governments globally. Flaherty forwards an idea of privacy as information control, "[i]ndividuals want to be left alone and to exercise some control over how information about them is used".[76]

Richard Posner and Lawrence Lessig focus on the economic aspects of personal information control. Posner criticizes privacy for concealing information, which reduces market efficiency. For Posner, employment is selling oneself in the labour market, which he believes is like selling a product. Any 'defect' in the 'product' that is not reported is fraud.[77] For Lessig, privacy breaches online can be regulated through code and law. Lessig claims "the protection of privacy would be stronger if people conceived of the right as a property right", and that "individuals should be able to control information about themselves".[78]

A collective value and a human right

There have been attempts to establish privacy as one of the fundamental human rights, whose social value is an essential component in the functioning of democratic societies.[79] Amitai Etzioni suggests a communitarian approach to privacy. This requires a shared moral culture for establishing social order.[80] Etzioni believes that "[p]rivacy is merely one good among many others",[81] and that technological effects depend on community accountability and oversight (ibid). He claims that privacy laws only increase government surveillance by weakening informal social controls.[82] Furthermore, the government is no longer the only or even principle threat to people's privacy. Etzioni notes that corporate data miners, or "Privacy Merchants (https://web.archive.org/web/20130905184715/http://icps.gwu.edu/files/2010/10/privacy-merchants.pdf)," stand to profit by selling massive dossiers of personal information, including purchasing decisions and Internet traffic, to the highest bidder. And while some might not find collection of private information objectionable when it is only used commercially by the private sector, the information these corporations amass and process is also available to the government, so that it is no longer possible to protect privacy by only curbing the State.[83]

Priscilla Regan believes that individual concepts of privacy have failed philosophically and in policy. She supports a social value of privacy with three dimensions: shared perceptions, public values, and collective components. Shared ideas about privacy allows freedom of conscience and diversity in thought. Public values guarantee democratic participation, including freedoms of speech and association, and limits government power. Collective elements describe privacy as collective good that cannot be divided. Regan's goal is to strengthen privacy claims in policy making: "if we did recognize the collective or public-good value of privacy, as well as the common and public value of privacy, those advocating privacy protections would have a stronger basis upon which to argue for its protection".[84]

Leslie Regan Shade argues that the human right to privacy is necessary for meaningful democratic participation, and ensures human dignity and autonomy. Privacy depends on norms for how information is distributed, and if this is appropriate. Violations of privacy depend on context. The human right to privacy has precedent in the United Nations Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[85] Shade believes that privacy must be approached from a people-centered perspective, and not through the marketplace.[86]

Dr. Eliza Watt, Westminster Law School, University of Westminster in London, UK, proposes application of the International Human Right Law (IHRL) concept of "virtual control" as an approach to deal with extraterritorial mass surveillance by state intelligence agencies.[87] Dr. Watt envisions the "virtual control" test, understood as a remote control over the individual's right to privacy of communications, where privacy is recognized under the ICCPR, Article 17. This, she contends, may help to close the normative gap that is being exploited by nation states.[88]

Privacy paradox and economic valuation

The *privacy paradox* is a phenomenon in which online users state that they are concerned about their privacy but behave as if they were not.[89] While this term was coined as early as 1998,[90] it wasn't used in its current popular sense until the year 2000.[91][89]

Susan B. Barnes similarly used the term *privacy paradox* to refer to the ambiguous boundary between private and public space on social media.[92] When compared to adults, young people tend to disclose more information on social media. However, this does not mean that they are not concerned about their privacy. Susan B. Barnes gave a case in her article: in a television interview about Facebook, a student addressed her concerns about disclosing personal information online. However, when the reporter asked to see her Facebook page, she put her home address, phone numbers, and pictures of her young son on the page.

The privacy paradox has been studied and scripted in different research settings. Although several studies have shown this inconsistency between privacy attitudes and behavior among online users, the reason for the paradox still remains unclear.[93] A main explanation for the privacy paradox is that users lack awareness of the risks and the degree of protection.[94] Users may underestimate the harm of disclosing information online. On the other hand, some researchers argue the privacy paradox comes from lack of technology literacy and from the design of sites.[95] For example, users may not know how to change their default settings even though they care about their privacy. Psychologists particularly pointed out that the privacy paradox occurs because users must trade-off between their privacy concerns and impression management.[96]

Research on irrational decision making

Some researchers believe that decision making takes place on an irrational level, especially when it comes to mobile computing. Mobile applications in particular are often built up in such a way that decision making is fast. Protection measures against these unconscious mechanisms are often difficult to access while downloading and installing apps. Even with mechanisms in place to protect user privacy, users may not have the knowledge or experience to enable these mechanisms.[97]

Users of mobile applications generally have very little knowledge of how their personal data are used. When they decide which application to download, they typically do not rely on the information provided by application vendors regarding the collection and use of personal data.[98] Other research finds that users are much more likely to be swayed by cost, functionality, design, ratings, reviews and number of downloads than requested permissions, regardless of how important users may claim permissions to be when asked.[99]

A study by Zafeiropoulou specifically examined location data, which is a form of personal information increasingly used by mobile applications.[100] Their survey also found evidence that supports the existence of privacy paradox for location data.[98] Privacy risk perception in relation to the use of privacy-enhancing technologies survey data indicates that a high perception of privacy risk is an insufficient motivator for people to adopt privacy protecting strategies, while knowing they exist.[98] It also raises a question on what the value of data is, as there is no equivalent of a stock-market for personal information.[101]

The economic valuation of privacy

The willingness to incur a privacy risk is suspected to be driven by a complex array of factors including risk attitudes, personal value for private information, and general attitudes to privacy (which may be derived from surveys).[102] One experiment aiming to determine the monetary value of several types of personal information indicated relatively low evaluations of personal information.[98]

Information asymmetry

Users are not always given the tools to live up to their professed privacy concerns, and they are sometimes willing to trade private information for convenience, functionality, or financial gain, even when the gains are very small.[103] One study suggests that people think their browser history is worth the equivalent of a cheap meal.[104] Another finds that attitudes to privacy risk do not appear to depend on whether it is already under threat or not.[102]

Inherent necessity for privacy violation

It is suggested that the privacy paradox should not be considered a paradox, but more of a *privacy dilemma*, for services that cannot exist without the user sharing private data.[104] However, the general public is typically not given the choice whether to share private data or not,[6] making it difficult to verify any claim that a service truly cannot exist without sharing private data.

Actions which reduce privacy

As with other conceptions of privacy, there are various ways to discuss what kinds of processes or actions remove, challenge, lessen, or attack privacy. In 1960 legal scholar William Prosser created the following list of activities which can be remedied with privacy protection:[105][106]

1. Intrusion into a person's private space, own affairs, or wish for solitude[105]
2. Public disclosure of personal information about a person which could be embarrassing for them to have revealed[105]
3. Promoting access to information about a person which could lead the public to have incorrect beliefs about them[105]
4. Encroaching someone's personality rights, and using their likeness to advance interests which are not their own[105]

From 2004 to 2008, building from this and other historical precedents, Daniel J. Solove presented another classification of actions which are harmful to privacy, including collection of information which is already somewhat public, processing of information, sharing information, and invading personal space to get private information.[107]

Collecting information

In the context of harming privacy, information collection means gathering whatever information can be obtained by doing something to obtain it.[107] Examples include surveillance and interrogation.[107] Another example is how consumers and marketers also collect information in the business context through facial recognition which has recently caused a concern for things such as privacy. There is currently research being done related to this topic.[108]

Aggregating information

It can happen that privacy is not harmed when information is available, but that the harm can come when that information is collected as a set, then processed together in such a way that the collective reporting of pieces of information encroaches on privacy.[109] Actions in this category which can lessen privacy include the following:[109]

- data aggregation, which is connecting many related but unconnected pieces of information[109]
- identification, which can mean breaking the de-identification of items of data by putting it through a de-anonymization process, thus making facts which were intended to not name particular people to become associated with those people[109]
- insecurity, such as lack of data security, which includes when an organization is supposed to be responsible for protecting data instead suffers a data breach which harms the people whose data it held[109]
- secondary use, which is when people agree to share their data for a certain purpose, but then the data is used in ways without the data donors' informed consent[109]
- exclusion is the use of a person's data without any attempt to give the person an opportunity to manage the data or participate in its usage[109]

Information dissemination

> *Count not him among your friends who will retail your privacies to the world.*
>
> — Publilius Syrus

Information dissemination is an attack on privacy when information which was shared in confidence is shared or threatened to be shared in a way that harms the subject of the information.[109]

There are various examples of this.[109] Breach of confidentiality is when one entity promises to keep a person's information private, then breaks that promise.[109] Disclosure is making information about a person more accessible in a way that harms the subject of the information, regardless of how the information was collected or the intent of making it available.[109] Exposure is a special type of disclosure in which the information disclosed is emotional to the subject or taboo to share, such as revealing their private life experiences, their nudity, or perhaps private body functions.[109] Increased accessibility means advertising the availability of information without actually distributing it, as in the case of doxxing.[109] Blackmail is making a threat to share information, perhaps as part of an effort to coerce someone.[109] Appropriation is an attack on the personhood of someone, and can include using the value of someone's reputation or likeness to advance interests which are not those of the person being appropriated.[109] Distortion is the creation of misleading information or lies about a person.[109]

Invasion

Invasion of privacy, a subset of expectation of privacy, is a different concept from the collecting, aggregating, and disseminating information because those three are a misuse of available data, whereas invasion is an attack on the right of individuals to keep personal secrets.[109] An invasion is an attack in which information, whether intended to be public or not, is captured in a way that insults the personal dignity and right to private space of the person whose data is taken.[109]

Intrusion

An *intrusion* is any unwanted entry into a person's private personal space and solitude for any reason, regardless of whether data is taken during that breach of space.[109] *Decisional interference* is when an entity somehow injects itself into the personal decision making process of another person, perhaps to influence that person's private decisions but in any case doing so in a way that disrupts the private personal thoughts that a person has.[109]

Examples of invasions of privacy

- In 2019, contract workers for Apple and Amazon reported being forced to continue listening to "intimate moments" captured on the companies' smart speakers in order to improve the quality of their automated speech recognition software.[6]

Techniques to improve privacy

Similarly to actions which reduce privacy, there are multiple angles of privacy and multiple techniques to improve them to varying extents. When actions are done at an organizational level, they may be referred to as cybersecurity.

Encryption

E-mails can be encrypted via S/MIME or PGP. The Signal app is notable for being available on many mobile devices and implementing a form of perfect forward secrecy.

Anonymity

Anonymizing proxies or anonymizing networks like I2P and Tor can be used to prevent the internet service providers from knowing which sites one visits and with whom one communicates.

User empowerment

Concrete solutions on how to solve paradoxical behavior still do not exist. Many efforts are focused on processes of decision making, like restricting data access permissions during application installation, but this would not completely bridge the gap between user intention and behavior. Susanne Barth and Menno D.T. de Jong believe that for users to make more conscious decisions on privacy matters, the design needs to be more user oriented.[97]

See also

- Civil liberties
- Digital identity
- Global surveillance
- Identity theft in the United States
- Open data
- Open access
- Privacy-enhancing technologies
- Privacy policy
- Solitude
- Transparency
- Wikipedia's privacy policy – Wikimedia Foundation

Works cited

- Solove, Daniel J. (2010). *Understanding Privacy*. Harvard University Press. ISBN 978-0674035072.

References

1. DeCew, Judith (2015-01-01). Zalta, Edward N. (ed.). *Privacy* (http://plato.stanford.edu/archives/spr2015/entries/privacy/) (Spring 2015 ed.).
2. "4 *Harvard Law Review* 193 (1890)" (http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html). Groups.csail.mit.edu. 1996-05-18. Retrieved 2019-08-22.
3. Information Privacy, Official Reference for the Certified Information privacy Professional (CIPP), Swire, 2007}}
4. Solove 2010, pp. 3–4.
5. "Privacy (Stanford Encyclopedia of Philosophy)" (http://plato.stanford.edu/entries/privacy/). plato.stanford. Retrieved 2012-01-01.
6. "Silicon Valley is Listening to Your Most Intimate Moments" (https://www.bloomberg.com/news/features/2019-12-11/silicon-valley-got-millions-to-let-siri-and-alexa-listen-in). Bloomberg Businessweek. 2019-12-11. Retrieved 2021-06-02.
7. "What I've Learned: Andy Grove" (http://www.esquire.com/features/what-ive-learned/learned-andy-grove-0500), *Esquire* Magazine, 1 May 2000
8. Jeffrey Rosen. "The Web Means the End of Forgetting" (https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=1&ref=technology) *New York Times*, July 19, 2010
9. "Facebook: active users worldwide" (https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/). *Statista*. Retrieved 2020-10-11.
10. Hugl, Ulrike (2011), "Reviewing Person's Value of Privacy of Online Social Networking," *Internet Research*, 21(4), in press, http://www.emeraldinsight.com/journals.htm?issn=1066-2243&volume=21&issue=4&articleid=1926600&show=abstract.
11. Kosinski, Michal; Stillwell, D.; Graepel, T. (2013). "Private traits and attributes are predictable from digital records of human behavior" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625324). *Proceedings of the National Academy of Sciences*. **110** (15): 5802–05. Bibcode:2013PNAS..110.5802K (https://ui.adsabs.harvard.edu/abs/2013PNAS..110.5802K). doi:10.1073/pnas.1218772110 (https://doi.org/10.1073%2Fpnas.1218772110). PMC 3625324 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625324). PMID 23479631 (https://pubmed.ncbi.nlm.nih.gov/23479631).
12. "Self-portraits and social media: The rise of the 'selfie' " (https://www.bbc.com/news/magazine-22511650). *BBC News*. 2013-06-07. Retrieved 2021-03-17.

13. Giroux, Henry A. (2015-05-04). "Selfie Culture in the Age of Corporate and State Surveillance". *Third Text*. **29** (3): 155–64. doi:10.1080/09528822.2015.1082339 (https://doi.org/10.1080%2F09528822.2015.1082339). ISSN 0952-8822 (https://www.worldcat.org/issn/0952-8822). S2CID 146571563 (https://api.semanticscholar.org/CorpusID:146571563).
14. Dhir, Amandeep; Torsheim, Torbjørn; Pallesen, Ståle; Andreassen, Cecilie S. (2017). "Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults?" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5440591). *Frontiers in Psychology*. **8**: 815. doi:10.3389/fpsyg.2017.00815 (https://doi.org/10.3389%2Ffpsyg.2017.00815). ISSN 1664-1078 (https://www.worldcat.org/issn/1664-1078). PMC 5440591 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5440591). PMID 28588530 (https://pubmed.ncbi.nlm.nih.gov/28588530).
15. Wong, Queenie. "Facebook takes down more than 3 billion fake accounts" (https://www.cnet.com/news/facebook-took-down-more-than-3-billion-fake-accounts/). *CNET*. Retrieved 2020-10-11.
16. de Montjoye, Yves-Alexandre; César A. Hidalgo; Michel Verleysen; Vincent D. Blondel (March 25, 2013). "Unique in the Crowd: The privacy bounds of human mobility" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607247). *Scientific Reports*. **3**: 1376. Bibcode:2013NatSR...3E1376D (https://ui.adsabs.harvard.edu/abs/2013NatSR...3E1376D). doi:10.1038/srep01376 (https://doi.org/10.1038%2Fsrep01376). PMC 3607247 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607247). PMID 23524645 (https://pubmed.ncbi.nlm.nih.gov/23524645).
17. Athanasios S. Voulodimos and Charalampos Z. Patrikakis, "Quantifying Privacy in Terms of Entropy for Context Aware Services", special issue of the Identity in the Information Society journal, "Identity Management in Grid and SOA", Springer, vol. 2, no 2, December 2009
18. "Sneaky tactics used by telemarketers and debt collectors to get your cell phone number" (http://www.businessinsider.com/sneaky-tactics-used-by-telemarketers-and-debt-collectors-to-get-your-cell-phone-number-2011-6). Businessinsider.com. Retrieved 2012-08-27.
19. "Getting Started – Sign in with Apple – Apple Developer" (https://developer.apple.com/sign-in-with-apple/get-started/). Apple Inc. Retrieved 2019-11-06.
20. "Android 10 privacy changes for accessing device location" (https://proandroiddev.com/android-q-privacy-changes-for-accessing-device-location-1c8e2197d0e2). ProAndroidDev. 2019-10-02. Retrieved 2019-11-06.
21. Popkin, Helen A.S., "Gov't officials want answers to secret iPhone tracking" (https://archive.today/20120714202126/http://technolog.msnbc.msn.com/_news/2011/04/21/6508416-govt-officials-want-answers-to-secret-iphone-tracking) *MSNBC*, "Technology", April 21, 2011
22. "Apple denies tracking iPhone users, but promises changes" (http://www.computerworld.com/s/article/9216210/Apple_denies_tracking_iPhone_users_but_promises_changes?taxonomyId=84), *Computerworld*, 27 April 2011
23. "Complaint for Injunctive and Other Relief" (https://www.azag.gov/sites/default/files/2021-05/Complaint%20%28redacted%29.pdf) (PDF). The Superior Court of the State of Arizona In and For the County of Maricopa. 2021-06-03. Retrieved 2021-06-03.
24. Kosinski, Michal; Stillwell, D.; Graepel, T. (2013). "Private traits and attributes are predictable from digital records of human behavior" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625324). *Proceedings of the National Academy of Sciences*. **110** (15): 5802–05. Bibcode:2013PNAS..110.5802K (https://ui.adsabs.harvard.edu/abs/2013PNAS..110.5802K). doi:10.1073/pnas.1218772110 (https://doi.org/10.1073%2Fpnas.1218772110). PMC 3625324 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625324). PMID 23479631 (https://pubmed.ncbi.nlm.nih.gov/23479631).
25. Federal Trade Commission (2010), "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," Preliminary FTC Staff Report (December), available at [1] (http://www.ftc.gov/os/2010/12/101201privacyreport.pdf).

26. Miyazaki, Anthony D. (2008), "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," *Journal of Public Policy & Marketing*, 23 (Spring), 19–33.
27. "The Italian Constitution" (https://web.archive.org/web/20161127152449/http://www.quirinale.it/qrnw/costituzione/pdf/costituzione_inglese.pdf) (PDF). The official website of the Presidency of the Italian Republic. Archived from the original (http://www.quirinale.it/page/costituzione) on 2016-11-27.
28. Solove 2010, p. 3.
29. Yael Onn, et al., *Privacy in the Digital Environment* (https://books.google.com/books?id=yeVRrrJw-zAC&pg=PA1), Haifa Center of Law & Technology, (2005) pp. 1–12
30. Quinn, Michael J. (2009). *Ethics for the Information Age*. ISBN 978-0-321-53685-3.
31. "Privacy Guidelines" (http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm). OECD. Retrieved 2019-08-22.
32. Cate, Fred H.; Collen, Peter; Mayer-Schönberger, Viktor. Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines (https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf) (PDF) (Report).
33. Jensen, Carlos (2004). *Privacy policies as decision-making tools: an evaluation of online privacy notices*. CHI (http://www.chi2004.org/index.html).
34. "Privacy Law" (https://www.oaic.gov.au/privacy-law/).
35. "For Your Information" (http://www.alrc.gov.au/publications/report-108). Alrc.gov.au. 2008-08-12. Retrieved 2019-08-22.
36. Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (https://www.comlaw.gov.au/Details/C2012A00197).
37. Burghardt, Buchmann, Böhm, Kühling, Sivridis *A Study on the Lack of Enforcement of Data Protection Acts* Proceedings of the 3rd int. conference on e-democracy, 2009.
38. Mark Scott (3 December 2014). "French Official Campaigns to Make 'Right to be Forgotten' Global" (https://bits.blogs.nytimes.com/2014/12/03/french-official-campaigns-to-make-right-to-be-forgotten-global/). nytimes. Retrieved 14 April 2018.
39. Masiero, Silvia (2018-09-24). "Explaining Trust in Large Biometric Infrastructures: A Critical Realist Case Study of India's Aadhaar Project" (https://dspace.lboro.ac.uk/2134/35413). *The Electronic Journal of Information Systems in Developing Countries*. **84** (6): e12053. doi:10.1002/isd2.12053 (https://doi.org/10.1002%2Fisd2.12053).
40. "Aadhaar: 7 changes transforming India in 2018" (https://www.gemalto.com/govt/customer-cases/aadhaar). *gemalto*. 2018-10-08.
41. Does Beckham judgment change rules? (http://news.bbc.co.uk/1/hi/uk/4482073.stm), from BBC News (retrieved 27 April 2005).
42. "Personal Information Toolkit" (http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/toolkit.pdf) Information Commissioner's Office, UK
43. "Fourth Amendment" (https://www.law.cornell.edu/wex/fourth_amendment). *LII / Legal Information Institute*. Retrieved 2021-03-20.
44. "The Privacy Act" (https://foia.state.gov/Learn/PrivacyAct.aspx). *Freedom of Information Act*. US Department of State. 2015-05-22. Retrieved 2015-11-19.
45. Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq.
46. Fourth Amendment to the United States Constitution
47. Visit to the United States of America (https://undocs.org/A/HRC/46/37/Add.4)
48. Solove 2010, pp. 15–17.
49. Warren and Brandeis, "The Right To Privacy" (http://www.law.louisville.edu/library/collections/brandeis/node/225)(1890) 4 Harvard Law Review 193
50. Solove 2010, p. 19.

51. Godkin, E.L. (December 1880). "Libel and its Legal Remedy" (http://digital.library.cornell.edu/cgi/t/text/pageviewer-idx?c=atla;cc=atla;rgn=full%20text;idno=atla0046-6;didno=atla0046-6;view=image;seq=0735;node=atla0046-6%3A1). *Atlantic Monthly*. **46** (278): 729–39.
52. Oulasvirta, Antti; Suomalainen, Tiia; Hamari, Juho; Lampinen, Airi; Karvonen, Kristiina (2014). "Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance" (https://www.researchgate.net/publication/264638054). *Cyberpsychology, Behavior, and Social Networking*. **17** (10): 633–38. doi:10.1089/cyber.2013.0585 (https://doi.org/10.1089%2Fcyber.2013.0585). PMID 25226054 (https://pubmed.ncbi.nlm.nih.gov/25226054).
53. Gavison, Ruth (1980). "Privacy and the Limits of Law". *Yale Law Journal*. **89** (3): 421–71. doi:10.2307/795891 (https://doi.org/10.2307%2F795891). JSTOR 795891 (https://www.jstor.org/stable/795891).
54. Bok, Sissela (1989). *Secrets : on the ethics of concealment and revelation* (Vintage Books ed.). New York: Vintage Books. pp. 10–11. ISBN 978-0-679-72473-5.
55. Solove 2010, p. 24.
56. The quotation is from Alan Westin.Westin, Alan F.; Blom-Cooper, Louis (1970). *Privacy and freedom*. London: Bodley Head. p. 7. ISBN 978-0-370-01325-1.
57. B.H.M., Custers; Metajuridica, Instituut voor. "Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination" (https://openaccess.leidenuniv.nl/handle/1887/46935). *openaccess.leidenuniv.nl*. Retrieved 2017-07-19. Note: this reference does not contain the quote (& the quote opens without closing).
58. Westin, Alan (1967). *Privacy and Freedom*. New York: Atheneum.
59. Hughes, Kirsty (2012). "A Behavioural Understanding of Privacy and Its Implications for Privacy Law". *The Modern Law Review*. **75** (5): 806–36. doi:10.1111/j.1468-2230.2012.00925.x (https://doi.org/10.1111%2Fj.1468-2230.2012.00925.x).
60. Solove 2010, p. 21.
61. Posner, Richard A. (1983). *The economics of justice* (https://archive.org/details/economi_pos_1981_00_0099/page/271) (5. print ed.). Cambridge, MA: Harvard University Press. p. 271 (https://archive.org/details/economi_pos_1981_00_0099/page/271). ISBN 978-0-674-23526-7.
62. Solove 2010, pp. 22–23.
63. Reiman, Jeffrey (1976). "Privacy, Intimacy, and Personhood". *Philosophy & Public Affairs*.
64. Benn, Stanley. "Privacy, freedom, and respect for persons". In Schoeman, Ferdinand (ed.). *Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press.
65. Kufer, Joseph (1987). "Privacy, Autonomy, and Self-Concept". *American Philosophical Quarterly*.
66. Goffman, Erving (1968). *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. New York: Doubleday.
67. Altman, Irwin (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey: Brooks/Cole Publishing Company.
68. Solove 2010, p. 35.
69. Rachels, James (Summer 1975). "Why Privacy is Important". *Philosophy & Public Affairs*. **4** (4): 323–33. JSTOR 2265077 (https://www.jstor.org/stable/2265077).
70. Citron, Danielle (2019). "Sexual Privacy" (https://scholarship.law.bu.edu/faculty_scholarship/620/). *Yale Law Journal*. **128**: 1877, 1880.
71. H. Jeff Smith (1994). *Managing Privacy: Information Technology and Corporate America* (https://archive.org/details/managingprivacyi0000smit). UNC Press Books. ISBN 978-0807821473.
72. "Fixing the Fourth Amendment with trade secret law: A response to Kyllo v. United States" (http://findarticles.com/p/articles/mi_qa3805/is_200206/ai_n9109326/pg_1). *Georgetown Law Journal*. 2002.

73. "Security Recommendations For Stalking Victims" (https://web.archive.org/web/20120111081006/http://www.privacyrights.org/fs/fs14a-stalking.htm). Privacyrights. 11 January 2012. Archived from the original (http://www.privacyrights.org/fs/fs14a-stalking.htm) on 11 January 2012. Retrieved 2 February 2008.
74. "FindLaw's Writ – Amar: Executive Privilege" (http://writ.corporate.findlaw.com/amar/20040416.html). Writ.corporate.findlaw.com. 2004-04-16. Retrieved 2012-01-01.
75. Popa, C., et. all., "Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy-Savvy Leaders", Carswell (2012), Ch. 6
76. Flaherty, D. (1989). Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, U.S.: The University of North Carolina Press.
77. Posner, R. A. (1981). "The economics of privacy". *The American Economic Review*. **71** (2): 405–09.
78. Lessig, L. (2006) Code: Version 2.0. New York, U.S.: Basic Books.
79. Johnson, Deborah (2009). Beauchamp; Bowie; Arnold (eds.). *Ethical theory and business* (8th ed.). Upper Saddle River, NJ: Pearson/Prentice Hall. pp. 428–42. ISBN 978-0-13-612602-7.
80. Etzioni, A. (2006). Communitarianism. In B. S. Turner (Ed.), The Cambridge Dictionary of Sociology (pp. 81–83). Cambridge, UK: Cambridge University Press.
81. Etzioni, A. (2007). Are new technologies the enemy of privacy? Knowledge, Technology & Policy, 20, 115–19.
82. Etzioni, A. (2000). A communitarian perspective on privacy. Connecticut Law Review, 32(3), 897–905.
83. Etzioni, Amitai (March 2012). "The Privacy Merchants: What is to be done?" (https://web.archive.org/web/20130905184715/http://icps.gwu.edu/files/2010/10/privacy-merchants.pdf) (PDF). *The Journal of Constitutional Law*. **14** (4): 950. Archived from the original (http://icps.gwu.edu/files/2010/10/privacy-merchants.pdf) (PDF) on 2013-09-05.
84. Regan, P. M. (1995). Legislating privacy: Technology, social values, and public policy. Chapel Hill, U.S.: The University of North Carolina Press.
85. "United Nations Universal Declaration of Human Rights" (https://web.archive.org/web/20141208080853/http://www.un.org/Overview/rights.html). 1948. Archived from the original (https://www.un.org/Overview/rights.html) on 2014-12-08.
86. Shade, L.R. (2008). Reconsidering the right to privacy in Canada. Bulletin of Science, Technology & Society, 28(1), 80–91.
87. Watt, Eliza. "The role of international human rights law in the protection of online privacy in the age of surveillance." In 2017 9th International Conference on Cyber Conflict (CyCon), pp. 1-14. IEEE, 2017. http://eprints.bournemouth.ac.uk/30324/1/THE%20ROLE%20OF%20INTERNATIONAL%20LAW%20CYCON%20TALLIN%202017.pdf
88. Watt, Eliza. "The role of international human rights law in the protection of online privacy in the age of surveillance." In 2017 9th International Conference on Cyber Conflict (CyCon), pp. 1-14. IEEE, 2017.
89. Swartz, J., "'Opting In': A Privacy Paradox", The Washington Post, 03 Sep 2000, H.1.
90. Bedrick, B., Lerner, B., Whitehead, B. "The privacy paradox: Introduction", "News Media and the Law", Washington, DC, Volume 22, Issue 2, Spring 1998, pp. P1–P3.
91. J. Sweat "Privacy paradox: Customers want control—and coupons", Information Week, Manhasset Iss, 781, April 10, 2000, p. 52.
92. "Volume 11, Number 9" (https://firstmonday.org/ojs/index.php/fm/issue/view/203). *firstmonday.org*. 4 September 2006. Retrieved 2019-11-25.

93. Taddicken, M (2014). "The 'Privacy Paradox'in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure" (https://doi.org/10.1111%2Fjcc4.12052). *Journal of Computer-Mediated Communication*. **19** (2): 248–73. doi:10.1111/jcc4.12052 (https://doi.org/10.1111%2Fjcc4.12052).
94. Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies* (pp. 36–58). Springer Berlin Heidelberg.
95. S. Livingstone (2008). "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression" (http://eprints.lse.ac.uk/27072/1/Taking_risky_opportunities_in_youthful_content_creation_%28LSERO%29.pdf) (PDF). *New Media & Society*. **10** (3): 393–411. doi:10.1177/1461444808089415 (https://doi.org/10.1177%2F1461444808089415). S2CID 31076785 (https://api.semanticscholar.org/CorpusID:31076785).
96. Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* article 1. [2] (http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1)
97. Barth, Susanne; de Jong, Menno D. T. (2017-11-01). "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review" (https://doi.org/10.1016%2Fj.tele.2017.04.013). *Telematics and Informatics*. **34** (7): 1038–58. doi:10.1016/j.tele.2017.04.013 (https://doi.org/10.1016%2Fj.tele.2017.04.013). ISSN 0736-5853 (https://www.worldcat.org/issn/0736-5853).
98. Kokolakis, Spyros (January 2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". *Computers & Security*. **64**: 122–34. doi:10.1016/j.cose.2015.07.002 (https://doi.org/10.1016%2Fj.cose.2015.07.002).
99. Barth, Susanne; de Jong, Menno D. T.; Junger, Marianne; Hartel, Pieter H.; Roppelt, Janina C. (2019-08-01). "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources" (https://doi.org/10.1016%2Fj.tele.2019.03.003). *Telematics and Informatics*. **41**: 55–69. doi:10.1016/j.tele.2019.03.003 (https://doi.org/10.1016%2Fj.tele.2019.03.003). ISSN 0736-5853 (https://www.worldcat.org/issn/0736-5853).
00. Zafeiropoulou, Aristea M.; Millard, David E.; Webber, Craig; O'Hara, Kieron (2013). "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?" (http://dl.acm.org/citation.cfm?doid=2464464.2464503). *Proceedings of the 5th Annual ACM Web Science Conference on – WebSci '13*. Paris: ACM Press: 463–472. doi:10.1145/2464464.2464503 (https://doi.org/10.1145%2F2464464.2464503). ISBN 978-1-4503-1889-1. S2CID 15732921 (https://api.semanticscholar.org/CorpusID:15732921).
01. Burkhardt, Kai. "The privacy paradox is a privacy dilemma" (https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma). *Internet Citizen*. Retrieved 2020-01-10.
02. Frik, Alisa; Gaudeul, Alexia (2020-03-27). "A measure of the implicit value of privacy under risk". *Journal of Consumer Marketing*. ahead-of-print (ahead-of-print): 457–72. doi:10.1108/JCM-06-2019-3286 (https://doi.org/10.1108%2FJCM-06-2019-3286). ISSN 0736-3761 (https://www.worldcat.org/issn/0736-3761).
03. Egelman, Serge; Felt, Adrienne Porter; Wagner, David (2013), "Choice Architecture and Smartphone Privacy: There's a Price for That", *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg, pp. 211–36, doi:10.1007/978-3-642-39498-0_10 (https://doi.org/10.1007%2F978-3-642-39498-0_10), ISBN 978-3-642-39497-3
04. "2. The Privacy Paradox", *Network Publicy Governance*, transcript Verlag, 2018, pp. 45–76, doi:10.14361/9783839442135-003 (https://doi.org/10.14361%2F9783839442135-003), ISBN 978-3-8394-4213-5
05. Solove 2010, p. 101.

06. Prosser, William (1960). "Privacy" (http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1). *California Law Review*. **48** (383): 389. doi:10.2307/3478805 (https://doi.org/10.2307%2F3478805). JSTOR 3478805 (https://www.jstor.org/stable/3478805).
07. Solove 2010, p. 103.
08. Zhou, Yinghui; Lu, Shasha; Ding, Min (2020-05-04). "Contour-as-Face Framework: A Method to Preserve Privacy and Perception" (https://doi.org/10.1177%2F0022243720920256). *Journal of Marketing Research*. **57** (4): 617–39. doi:10.1177/0022243720920256 (https://doi.org/10.1177%2F0022243720920256). ISSN 0022-2437 (https://www.worldcat.org/issn/0022-2437). S2CID 218917353 (https://api.semanticscholar.org/CorpusID:218917353).
09. Solove 2010, pp. 104–05.

External links

- Glenn Greenwald: Why privacy matters (https://www.youtube.com/watch?v=pcSlowAhvUk). Video on YouTube, provided by TED. Published 10 October 2014.
- International Privacy Index world map (https://chartsbin.com/view/by8), *The 2007 International Privacy Ranking*, Privacy International (London).
- "Privacy" (http://plato.stanford.edu/entries/privacy/) entry in the Stanford Encyclopedia of Philosophy.