Privacy

Privacy (UK: /ˈprɪvəsiː/, US: /ˈpraɪ-/)[1][2] is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

Banksy's *One Nation Under CCTV* graffiti, adjacent to an actual CCTV camera

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.

Throughout history, there have been various conceptions of privacy. Most cultures acknowledge the right of individuals to keep aspects of their personal lives out of the public domain. The right to be free from unauthorized invasions of privacy by governments, corporations, or individuals is enshrined in the privacy laws of many countries and, in some instances, their constitutions.

With the rise of technology, the debate regarding privacy has expanded from a bodily sense to include a digital sense. In most countries, the right to digital privacy is considered an extension of the original right to privacy, and many countries have passed acts that further protect digital privacy from public and private entities.

There are multiple techniques to invade privacy, which may be employed by corporations or governments for profit or political reasons. Conversely, in order to protect privacy, people may employ encryption or anonymity measures.

Etymology

The word privacy is derived from the Latin word and concept of '*privatus*', which referred to things set apart from what is public; personal and belonging to oneself, and not to the state.[3] Literally, '*privatus*' is the past participle of the Latin verb '*privere*' meaning 'to be deprived of'. [4]

History

Philosophical views on privacy

The concept of privacy has been explored and discussed by numerous philosophers throughout 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.[5] Privacy is valued along with other basic necessities of life in the Jewish deutero-canonical Book of Sirach.[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.

English philosopher John Locke's (1632-1704) writings on natural rights and the social contract laid the groundwork for modern conceptions of individual rights, including the right to privacy. In his *Second Treatise of Civil Government*(1689), Locke argued that a man is entitled to his own self through one's natural rights of life, liberty, and property.[7] He believed that the government was responsible for protecting these rights so individuals were guaranteed private spaces to practice personal activities.[8]

In the political sphere, philosophers hold differing views on the right of private judgment. German philosopher Georg Wilhelm Friedrich Hegel (1770-1831) makes the distinction between *moralität*, which refers to an individual's private judgment, and *sittlichkeit*, pertaining to one's rights and obligations as defined by an existing corporate order. On the contrary, Jeremy Bentham (1748-1832), an English philosopher, interpreted law as an invasion of privacy. His theory of utilitarianism argued that legal actions should be judged by the extent of their contribution to human wellbeing, or necessary utility.[9]

Hegel's notions were modified by prominent 19th century English philosopher John Stuart Mill. Mill's essay *On Liberty* (1859) argued for the importance of protecting individual liberty against the tyranny of the majority and the interference of the state. His views emphasized the right of privacy as essential for personal development and self-expression.[10]

Discussions surrounding surveillance coincided with philosophical ideas on privacy. Jeremy Bentham developed the phenomenon known as the Panoptic effect through his 1791 architectural design of a prison called Panopticon. The phenomenon explored the possibility of surveillance as a general awareness of being watched that could never be proven at any particular moment.[11] French philosopher Michel Foucault (1926-1984) concluded that the possibility of surveillance in the instance of the Panopticon meant a prisoner had no choice but to conform to the prison's rules.[11]

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",[12] and that it was written mainly in response to the increase in newspapers and photographs made possible by printing technologies.[13]

In 1948, *1984*, written by George Orwell, was published. A classic dystopian novel, *1984* describes the life of Winston Smith in 1984, located in Oceania, a totalitarian state. The all-controlling Party, the party in power led by Big Brother, is able to control power through mass surveillance and limited freedom of speech and thought. George Orwell provides commentary on the negative effects of totalitarianism, particularly on privacy and censorship.[14] Parallels have been drawn between *1984* and modern censorship and privacy, a notable example being that large social media companies, rather than the government, are able to monitor a user's data and decide what is allowed to be said online through their censorship policies, ultimately for monetary purposes.[15]

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.

In the 1960s, people began to consider how changes in technology were bringing changes in the concept of privacy.[16] Vance Packard's *The Naked Society* was a popular book on privacy from that era and led US discourse on privacy at that time.[16] In addition, Alan Westin's *Privacy and Freedom* shifted the debate regarding privacy from a physical sense, how the government controls a person's body (i.e. *Roe v. Wade*) and other activities such as wiretapping and photography. As important records became digitized, Westin argued that personal data was becoming too accessible and that a person should have complete jurisdiction over their data, laying the foundation for the modern discussion of privacy.[17]

New technologies can also create new ways to gather private information. In 2001, the legal case *Kyllo v. United States* (533 U.S. 27) determined that the use of thermal imaging devices that can reveal previously unknown information without a warrant constitutes a violation of privacy. 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.[18]

Police and government

Police and citizens often conflict on what degree the police can intrude a citizen's digital privacy. For instance, in 2012, the Supreme Court ruled unanimously in *United States v. Jones* (565 U.S. 400), in the case of Antoine Jones who was arrested of drug possession using a GPS tracker on his car that was placed without a warrant, that warrantless tracking infringes the Fourth Amendment. The Supreme Court also justified that there is some "reasonable expectation of privacy" in transportation since the reasonable expectation of privacy had already been established under *Griswold v. Connecticut* (1965). The Supreme Court also further clarified that the Fourth Amendment did not only pertain to physical instances of intrusion but also digital instances, and thus *United States v. Jones* became a landmark case.[19]

In 2014, the Supreme Court ruled unanimously in *Riley v. California* (573 U.S. 373), where David Leon Riley was arrested after he was pulled over for driving on expired license tags when the police searched his phone and discovered that he was tied to a shooting, that searching a citizen's phone without a warrant was an unreasonable search, a violation of the Fourth Amendment. The Supreme Court concluded that the cell phones contained personal information different from trivial items, and went beyond to state that

information stored on the cloud was not necessarily a form of evidence. *Riley v. California* evidently became a landmark case, protecting the digital protection of citizen's privacy when confronted with the police.[20]

A recent notable occurrence of the conflict between law enforcement and a citizen in terms of digital privacy has been in the 2018 case, *Carpenter v. United States* (585 U.S. ____). In this case, the FBI used cell phone records without a warrant to arrest Timothy Ivory Carpenter on multiple charges, and the Supreme Court ruled that the warrantless search of cell phone records violated the Fourth Amendment, citing that the Fourth Amendment protects "reasonable expectations of privacy" and that information sent to third parties still falls under data that can be included under "reasonable expectations of privacy".[21]

Beyond law enforcement, many interactions between the government and citizens have been revealed either lawfully or unlawfully, specifically through whistleblowers. One notable example is Edward Snowden, who released multiple operations related to the mass surveillance operations of the National Security Agency (NSA), where it was discovered that the NSA continues to breach the security of millions of people, mainly through mass surveillance programs whether it was collecting great amounts of data through third party private companies, hacking into other embassies or frameworks of international countries, and various breaches of data, which prompted a culture shock and stirred international debate related to digital privacy.[22]

Internet

The Internet and technologies built on it enable new forms of social interactions at increasingly faster speeds and larger scales. Because the computer networks which underlie the Internet introduce such a wide range of novel security concerns, the discussion of *privacy* on the Internet is often conflated with *security*.[23] Indeed, many entities such as corporations involved in the surveillance economy inculcate a security-focused conceptualization of privacy which reduces their obligations to uphold privacy into a matter of regulatory compliance,[24] while at the same time lobbying to minimize those regulatory requirements.[25]

The Internet's effect on privacy includes all of the ways that computational technology and the entities that control it can subvert the privacy expectations of their users.[26][27] In particular, the right to be forgotten is motivated by both the *computational ability* to store and search through massive amounts of data as well as the *subverted expectations* of users who share information online without expecting it to be stored and retained indefinitely. Phenomena such as revenge porn and deepfakes are not merely individual because they require both the ability to obtain images without someone's consent as well as the social and economic infrastructure to disseminate that content widely.[28] Therefore, privacy advocacy groups such as the Cyber Civil Rights Initiative and the Electronic Frontier Foundation argue that addressing the new privacy harms introduced by the Internet requires both technological improvements to encryption and anonymity as well as societal efforts such as legal regulations to restrict corporate and government power.[29][30]

While the Internet began as a government and academic effort up through the 1980s, private corporations began to enclose the hardware and software of the Internet in the 1990s, and now most Internet infrastructure is owned and managed by for-profit corporations.[31] As a result, the ability of governments to protect their citizens' privacy is largely restricted to industrial policy, instituting controls on

corporations that handle communications or personal data.[32][33] Privacy regulations are often further constrained to only protect specific demographics such as children,[34] or specific industries such as credit card bureaus.[35]

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[36] 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.[26]

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".[37] 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.[38]

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 candidates 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.[26]

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.[39] However, due to modern corporate and governmental surveillance, this may pose a risk to privacy.[40] 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.[41]

Online harassment

An invasion of someone's privacy may be widely and quickly disseminated over the Internet. When social media sites and other online communities fail to invest in content moderation, an invasion of privacy can expose people to a much greater volume and degree of harassment than would otherwise be possible. Revenge porn may lead to misogynist or homophobic harassment, such as in the suicide of Amanda Todd and the suicide of Tyler Clementi. When someone's physical location or other sensitive information is leaked over the Internet via doxxing, harassment may escalate to direct physical harm such as stalking or swatting.

Despite the way breaches of privacy can magnify online harassment, online harassment is often used as a justification to curtail freedom of speech, by removing the expectation of privacy via anonymity, or by enabling law enforcement to invade privacy without a search warrant. In the wake of Amanda Todd's death, the Canadian parliament proposed a motion purporting to stop bullying, but Todd's mother herself gave testimony to parliament rejecting the bill due to its provisions for warrantless breaches of privacy, stating "I don't want to see our children victimized again by losing privacy rights."[42][43][44]

Even where these laws have been passed despite privacy concerns, they have not demonstrated a reduction in online harassment. When the Korea Communications Commission introduced a registration system for online commenters in 2007, they reported that malicious comments only decreased by 0.9%, and in 2011 it was repealed.[45] A subsequent analysis found that the set of users who posted the most comments actually increased the number of "aggressive expressions" when forced to use their real name.[46]

In the US, while federal law only prohibits online harassment based on protected characteristics such as gender and race,[47] individual states have expanded the definition of harassment to further curtail speech: Florida's definition of online harassment includes "any use of data or computer software" that "Has the effect of substantially disrupting the orderly operation of a school."[48]

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, and their improper use violates that user's privacy. A recent MIT study by de Montjoye et al. showed that four spatio-temporal points constituting 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 confer little privacy protection.[49]

Several methods to protect user privacy in location-based services have been proposed, including the use of anonymizing servers and blurring of information. Methods to quantify privacy have also been proposed, to calculate the equilibrium between the benefit of obtaining accurate location information and the risks of breaching an individual's privacy.[50]

Ethical controversies over location privacy

There have been scandals regarding location privacy. One instance was the scandal concerning AccuWeather, where it was revealed that AccuWeather was selling locational data. This consisted of a user's locational data, even if they opted out within Accuweather, which tracked users' location. Accuweather sold this data to Reveal Mobile, a company that monetizes data related to a user's location.[51] Other international cases are similar to the Accuweather case. In 2017, a leaky API inside the McDelivery App exposed private data, which consisted of home addresses, of 2.2 million users.[52]

In the wake of these types of scandals, many large American technology companies such as Google, Apple, and Facebook have been subjected to hearings and pressure under the U.S. legislative system. In 2011, US Senator Al Franken wrote an open letter to Steve Jobs, noting the ability of iPhones and iPads to record and store users' locations in unencrypted files.[53][54] Apple claimed this was an unintentional software bug, but Justin Brookman of the Center for Democracy and Technology directly challenged that

portrayal, stating "I'm glad that they are fixing what they call bugs, but I take exception with their strong denial that they track users."[55] In 2021, the U.S. state of Arizona found in a court case that Google misled its users and stored the location of users regardless of their location settings.[56]

Advertising

The Internet has become a significant medium for advertising, with digital marketing making up approximately half of the global ad spending in 2019.[57] While websites are still able to sell advertising space without tracking, including via contextual advertising, digital ad brokers such as Facebook and Google have instead encouraged the practice of behavioral advertising, providing code snippets used by website owners to track their users via HTTP cookies. This tracking data is also sold to other third parties as part of the mass surveillance industry. Since the introduction of mobile phones, data brokers have also been planted within apps, resulting in a $350 billion digital industry especially focused on mobile devices.[58]

Digital privacy has become the main source of concern for many mobile users, especially with the rise of privacy scandals such as the Facebook–Cambridge Analytica data scandal.[58] Apple has received some reactions for features that prohibit advertisers from tracking a user's data without their consent.[59] Google attempted to introduce an alternative to cookies named FLoC which it claimed reduced the privacy harms, but it later retracted the proposal due to antitrust probes and analyses that contradicted their claims of privacy.[60][61][62]

Metadata

The ability to do online inquiries about individuals has expanded dramatically over the last decade. Importantly, directly observed behavior, 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.[63]

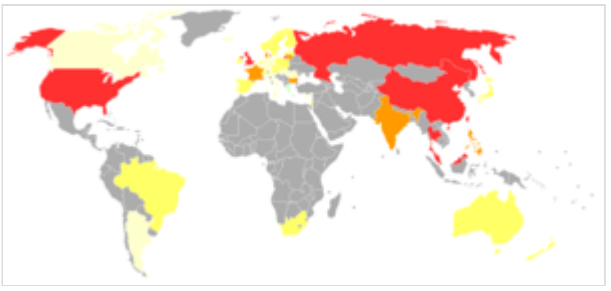
In Australia, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 made a distinction between collecting the contents of messages sent between users and the metadata surrounding those messages.

Legal right to privacy

Most countries give citizens rights to privacy in their constitutions.[16] 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."[16] The Italian Constitution also defines the right to privacy.[64] Among most countries whose constitutions do not explicitly describe privacy rights, court decisions have interpreted their constitutions to intend to give privacy rights.[16]

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.[16]

Beyond national privacy laws, there are international privacy agreements.[65] The United Nations Universal Declaration of Human Rights says "No one shall be subjected to arbitrary interference with [their] privacy, family, home or correspondence, nor to attacks upon [their] honor and reputation."[16] 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.[16] The 2004 Privacy Framework by the Asia-Pacific Economic Cooperation is a privacy protection agreement for the members of that organization.[16]



Privacy International 2007 privacy ranking. On one end of the spectrum, green indicates countries that uphold human rights standards while on the other end, red indicates countries considered endemic surveillance societies. This ranking was the last global report conducted by Privacy International, and it is demonstrated that countries that do have the legal right to privacy explicitly mentioned in their constitutions trend closer to yellow and green while those that do not trend closer to red.

Free market vs consumer protection

Approaches to privacy can, broadly, be divided into two categories: free market or consumer protection.[66]

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.[67] The principles reflected in the guidelines, free of legislative interference, are analyzed in an article putting them into perspective with concepts of the GDPR put into law later in the European Union.[68]

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.[69]

By country

Australia

The *Privacy Act 1988* is administered by the Office of the Australian Information Commissioner. 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.[70]

In 2008 the Australian Law Reform Commission (ALRC) conducted a review of Australian privacy law and produced a report titled "For Your Information".[71] Recommendations were taken up and implemented by the Australian Government via the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.[72]

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.

Canada

Canada is a federal state whose provinces and territories abide by the common law save the province of Quebec whose legal tradition is the civil law. Privacy in Canada was first addressed through the *Privacy Act*,[73] a 1985 piece of legislation applicable to personal information held by government institutions. The provinces and territories would later follow suit with their own legislation. Generally, the purposes of said legislation are to provide individuals rights to access personal information; to have inaccurate personal information corrected; and to prevent unauthorized collection, use, and disclosure of personal information.[74] In terms of regulating personal information in the private sector, the federal *Personal Information Protection and Electronic Documents Act* [75] ("PIPEDA") is enforceable in all jurisdictions unless a substantially similar provision has been enacted on the provincial level.[76] However, inter-provincial or international information transfers still engage PIPEDA.[76] PIPEDA has gone through two law overhaul efforts in 2021 and 2023 with the involvement of the Office of the Privacy Commissioner and Canadian academics.[77] In the absence of a statutory private right of action absent an OPC investigation, the common law torts of intrusion upon seclusion and public disclosure of private facts, as well as the Civil Code of Quebec may be brought for an infringement or violation of privacy.[78][79] Privacy is also protected under ss. 7 and 8 of the *Canadian Charter of Rights and Freedoms*[80] which is typically applied in the criminal law context.[81] In Quebec, individuals' privacy is safeguarded by articles 3 and 35 to 41 of the Civil Code of Quebec[82] as well as by s. 5 of the Charter of human rights and freedoms.[83]

European Union

In 2016, the European Union passed the General Data Protection Regulation (GDPR), which was intended to reduce the misuse of personal data and enhance individual privacy, by requiring companies to receive consent before acquiring personal information from users.[84]

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.[85] The European Union also champions the Right to be Forgotten concept in support of its adoption by other countries.[86]

India

Since the introduction of the Aadhaar project in 2009, which resulted in all 1.2 billion Indians being associated with a 12-digit biometric-secured number. Aadhaar has uplifted the poor in India by providing them with a form of identity and preventing the fraud and waste of resources, as normally the government would not be able to allocate its resources to its intended assignees due to the ID issues. With the rise of Aadhaar, India has debated whether Aadhaar violates an individual's privacy and whether any organization should have access to an individual's digital profile, as the Aadhaar card became associated

with other economic sectors, allowing for the tracking of individuals by both public and private bodies.[87] Aadhaar databases have suffered from security attacks as well and the project was also met with mistrust regarding the safety of the social protection infrastructures.[88] In 2017, where the Aadhar was challenged, the Indian Supreme Court declared privacy as a human right, but postponed the decision regarding the constitutionality of Aadhaar for another bench.[89] In September 2018, the Indian Supreme Court determined that the Aadhaar project did not violate the legal right to privacy.[90]

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.[91] 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.[92]

United States

In the United States, more systematic treatises of privacy did not appear until the 1890s, with the development of privacy law in America.[93] Although the US Constitution does not explicitly include the right to privacy, individual as well as locational privacy may be implicitly granted by the Constitution under the 4th Amendment.[94] 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* and *Roe v. Wade*. *Dobbs v. Jackson Women's Health Organization* later overruled *Roe v. Wade*, with Supreme Court Justice Clarence Thomas characterizing *Griswold*'s penumbral argument as having a "facial absurdity",[95] casting doubt on the validity of a constitutional right to privacy in the United States and of previous decisions relying on it.[96] 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.[97] Certain privacy rights have been established in the United States via legislation such as the Children's Online Privacy Protection Act (COPPA),[98] the Gramm–Leach–Bliley Act (GLB), and the Health Insurance Portability and Accountability Act (HIPAA). [99]

Unlike the EU and most EU-member states, the US does not recognize the right to privacy of non-US citizens. The UN's Special Rapporteur on the right to privacy, Joseph A. Cannataci, criticized this distinction.[100]

Conceptions of privacy

Privacy as contextual integrity

The theory of contextual integrity,[101] developed by Helen Nissenbaum, defines privacy as an appropriate information flow, where appropriateness, in turn, is defined as conformance with legitimate, informational norms specific to social contexts.

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.[102] 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.[103]

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.[102] 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.[102]

Limited access

Limited access refers to a person's ability to participate in society without having other individuals and organizations collect information about them.[104]

Various theorists have imagined privacy as a system for limiting access to one's personal information.[104] 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."[104][105] Adopting an approach similar to the one presented by Ruth Gavison[106] Nine years earlier,[107] Sissela Bok said that privacy is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention."[104][108]

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.[109][110] 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.[111][112]

States of privacy

Alan Westin defined four states—or experiences—of privacy: solitude, intimacy, anonymity, and reserve. Solitude is a physical separation from others;[113] 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.[113] Anonymity is the "desire of individuals for times of 'public privacy.'"[113] 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 themself.[113]

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.[114] (In this sense, "accessing" an individual includes accessing personal information about them.)[114] Behavioral barriers communicate to others—verbally, through language, or non-verbally, through personal space, body language, or clothing—that an individual does not want the other person to access or experience them.[114] Lastly, normative barriers, such as laws and social norms, restrain others from attempting to access or experience an individual.[114]

Privacy as personal control

Psychologist Carl A. Johnson has identified the psychological concept of “personal control” as closely tied to privacy. His concept was developed as a process containing four stages and two behavioural outcome relationships, with one’s outcomes depending on situational as well as personal factors.[115] Privacy is described as “behaviors falling at specific locations on these two dimensions”.[116]

Johnson examined the following four stages to categorize where people exercise personal control: outcome choice control is the selection between various outcomes. Behaviour selection control is the selection between behavioural strategies to apply to attain selected outcomes. Outcome effectance describes the fulfillment of selected behaviour to achieve chosen outcomes. Outcome realization control is the personal interpretation of one’s achieved outcome. The relationship between two factors– primary and secondary control, is defined as the two-dimensional phenomenon where one reaches personal control: primary control describes behaviour directly causing outcomes, while secondary control is behaviour indirectly causing outcomes.[117] Johnson explores the concept that privacy is a behaviour that has secondary control over outcomes.

Lorenzo Magnani expands on this concept by highlighting how privacy is essential in maintaining personal control over one's identity and consciousness.[118] He argues that consciousness is partly formed by external representations of ourselves, such as narratives and data, which are stored outside the body. However, much of our consciousness consists of internal representations that remain private and are rarely externalized. This internal privacy, which Magnani refers to as a form of "information property" or "moral capital," is crucial for preserving free choice and personal agency. According to Magnani,[119] when too much of our identity and data is externalized and subjected to scrutiny, it can lead to a loss of personal control, dignity, and responsibility. The protection of privacy, therefore, safeguards our ability to develop and pursue personal projects in our own way, free from intrusive external forces.

Acknowledging other conceptions of privacy while arguing that the fundamental concern of privacy is behavior selection control, Johnson converses with other interpretations including those of Maxine Wolfe and Robert S. Laufer, and Irwin Altman. He clarifies the continuous relationship between privacy and personal control, where outlined behaviours not only depend on privacy, but the conception of one’s privacy also depends on his defined behavioural outcome relationships.[120]

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".[121][122]

In various legal contexts, when privacy is described as secrecy, a conclusion is reached: if privacy is secrecy, then rights to privacy do not apply for any information which is already publicly disclosed.[123] 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.[123]

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 their physical and mental reality and a moral right to self-determination.[124] Through the "social ritual" of privacy, or the social practice of respecting an individual's privacy barriers, the social group communicates to developing children that they have exclusive moral rights to their bodies—in other words, moral ownership of their body.[124] 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.[124]

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.[125] Privacy is required to exercise choice.[125] Overt observation makes the individual aware of himself or herself as an object with a "determinate character" and "limited probabilities."[125] Covert observation, on the other hand, changes the conditions in which the individual is exercising choice without his or her knowledge and consent.[125]

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.[126] Furthermore, others must acknowledge and respect the self's boundaries—in other words, they must respect the individual's privacy.[126]

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.[126] In addition, studies of adults in particular institutions, such as Erving Goffman's study of "total institutions" such as prisons and mental institutions,[127] suggest that systemic and routinized deprivations or violations of privacy deteriorate one's sense of autonomy over time.[126]

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]."[128] This control primarily entails the ability to regulate contact with others.[128] 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.[128]

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.[126] Such self-discovery and self-criticism contributes to one's understanding of oneself and shapes one's sense of identity.[126]

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.[129] 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.[129]

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."[129][130] 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.[131]

Physical privacy

Physical privacy could be defined as preventing "intrusions into one's physical space or solitude."[132] 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".[133]

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.[134] There are different things that can be prevented to protect one's physical privacy, including people watching (even through recorded images) one's intimate behaviours or intimate parts and unauthorized access to one's personal possessions or places. Examples of possible efforts used to avoid the former, especially for modesty reasons, are clothes, walls, fences, privacy screens, cathedral glass, window coverings, etc.

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[135] or declare certain information to be classified, or a corporation might attempt to protect valuable proprietary information as trade secrets.[133]

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.[136]

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".[137]

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.[138] 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",[139] and that "individuals should be able to control information about themselves".[140]

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.[141]

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".[142]

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."[143] Shade believes that privacy must be approached from a people-centered perspective, and not through the marketplace.[144]

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. 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.[145]

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.[146] While this term was coined as early as 1998,[147] it was not used in its current popular sense until the year 2000.[148][146]

Susan B. Barnes similarly used the term *privacy paradox* to refer to the ambiguous boundary between private and public space on social media.[149] 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. Several studies have shown this inconsistency between privacy attitudes and behavior among online users.[150] However, by now an increasing number of studies have also shown that there are significant and at times large correlations between privacy concerns and information sharing behavior,[151] which speaks against the privacy paradox. A meta-analysis of 166 studies published on the topic reported an overall small but significant relation between privacy concerns and informations sharing or use of privacy protection measures.[152] So although there are several individual instances or anecdotes where behavior appear paradoxical, on average privacy concerns and privacy behaviors seem to be related, and several findings question the general existence of the privacy paradox.[153]

However, the relationship between concerns and behavior is likely only small, and there are several arguments that can explain why that is the case. According to the attitude-behavior gap, attitudes and behaviors are *in general* and in most cases not closely related.[154] A main explanation for the partial mismatch in the context of privacy specifically is that users lack awareness of the risks and the degree of protection.[155] Users may underestimate the harm of disclosing information online.[156] On the other hand, some researchers argue that the mismatch comes from lack of technology literacy and from the design of sites.[157] For example, users may not know how to change their default settings even though they care about their privacy. Psychologists Sonja Utz and Nicole C. Krämer particularly pointed out that the privacy paradox can occur when users must trade-off between their privacy concerns and impression management.[158]

Research on irrational decision making

A study conducted by Susanne Barth and Menno D.T. de Jo demonstrates 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 spurs decision making that is fast and automatic without

assessing risk factors. 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.[159]

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 are not able to effectively interpret the information provided by application vendors regarding the collection and use of personal data.[160] Other research finds that this lack of interpretability means users are much more likely to be swayed by cost, functionality, design, ratings, reviews and number of downloads than requested permissions for usage of their personal data.[161]

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 are typically measured using surveys).[162] One experiment aiming to determine the monetary value of several types of personal information indicated relatively low evaluations of personal information.[160] Despite claims that ascertaining the value of data requires a "stock-market for personal information",[163] surveillance capitalism and the mass surveillance industry regularly place price tags on this form of data as it is shared between corporations and governments.

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.[164] One study suggests that people think their browser history is worth the equivalent of a cheap meal.[165] Another finds that attitudes to privacy risk do not appear to depend on whether it is already under threat or not.[162] The methodology of user empowerment describes how to provide users with sufficient context to make privacy-informed decisions.

Inherent necessity for privacy violation

It is suggested by Andréa Belliger and David J. Krieger 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.[165] However, the general public is typically not given the choice whether to share private data or not,[18][56] making it difficult to verify any claim that a service truly cannot exist without sharing private data.

Privacy calculus model

The privacy calculus model posits that two factors determine privacy behavior, namely privacy concerns (or perceived risks) and expected benefits.[166][167] By now, the privacy calculus has been supported by several studies.[168][169]

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:[170][171]

1. Intrusion into a person's private space, own affairs, or wish for solitude[170]
2. Public disclosure of personal information about a person which could be embarrassing for them to have revealed[170]
3. Promoting access to information about a person which could lead the public to have incorrect beliefs about them[170]
4. Encroaching someone's personality rights, and using their likeness to advance interests which are not their own[170]

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.[172]

Collecting information

In the context of harming privacy, information collection means gathering whatever information can be obtained by doing something to obtain it.[172] Examples include surveillance and interrogation.[172] 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.[173]

Companies like Google and Meta collect vast amounts of personal data from their users through various services and platforms. This data includes browsing habits, search history, location information, and even personal communications. These companies then analyze and aggregate this data to create detailed user profiles, which are sold to advertisers and other third parties. This practice is often done without explicit user consent, leading to an invasion of privacy as individuals have little control over how their information is used. The sale of personal data can result in targeted advertising, manipulation, and even potential security risks, as sensitive information can be exploited by malicious actors. This commercial exploitation of personal data undermines user trust and raises significant ethical and legal concerns regarding data protection and privacy rights. [174]

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.[175] Actions in this category which can lessen privacy include the following:[175]

- data aggregation, which is connecting many related but unconnected pieces of information[175]
- 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[175]
- 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[175]
- 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[175]
- 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[175]

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.[175]

There are various examples of this.[175] Breach of confidentiality is when one entity promises to keep a person's information private, then breaks that promise.[175] 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.[175] 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.[175] Increased accessibility means advertising the availability of information without actually distributing it, as in the case of doxing.[175] Blackmail is making a threat to share information, perhaps as part of an effort to coerce someone.[175] 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.[175] Distortion is the creation of misleading information or lies about a person.[175]

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.[175] 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.[175]

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.[175] *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.[175]

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.[18]

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

Individuals can encrypt e-mails via enabling either two encryption protocols, S/MIME, which is built into companies like Apple or Outlook and thus most common, or PGP.[176] The Signal messaging app, which encrypts messages so that only the recipient can read the message, is notable for being available on many mobile devices and implementing a form of perfect forward secrecy.[177] Signal has received praise from whistleblower Edward Snowden.[178] Encryption and other privacy-based security measures are also used in some cryptocurrencies such as Monero and ZCash.[179][180]

Anonymity

Anonymizing proxies or anonymizing networks like I2P and Tor can be used to prevent Internet service providers (ISP) from knowing which sites one visits and with whom one communicates, by hiding IP addresses and location, but does not necessarily protect a user from third party data mining. Anonymizing proxies are built into a user's device, in comparison to a Virtual Private Network (VPN), where users must download software.[181] Using a VPN hides all data and connections that are exchanged between servers and a user's computer, resulting in the online data of the user being unshared and secure, providing a barrier between the user and their ISP, and is especially important to use when a user is connected to public Wi-Fi. However, users should understand that all their data does flow through the VPN's servers rather than the ISP. Users should decide for themselves if they wish to use either an anonymizing proxy or a VPN.

In a more non-technical sense, using incognito mode or private browsing mode will prevent a user's computer from saving history, Internet files, and cookies, but the ISP will still have access to the users' search history. Using anonymous search engines will not share a user's history, clicks, and will obstruct ad blockers.[182]

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.[159]

Other security measures

In a social sense, simply limiting the amount of personal information that users posts on social media could increase their security, which in turn makes it harder for criminals to perform identity theft.[182] Moreover, creating a set of complex passwords and using two-factor authentication can allow users to be less susceptible to their accounts being compromised when various data leaks occur. Furthermore, users should protect their digital privacy by using anti-virus software, which can block harmful viruses like a pop-up scanning for personal information on a users' computer.[183]

Legal methods

Although there are laws that promote the protection of users, in some countries, like the U.S., there is no federal digital privacy law and privacy settings are essentially limited by the state of current enacted privacy laws. To further their privacy, users can start conversing with representatives, letting representatives know that privacy is a main concern, which in turn increases the likelihood of further privacy laws being enacted.[184]

Privacy in non-human animals

David Attenborough, a biologist and natural historian, affirmed that gorillas "value their privacy" while discussing a brief escape by a gorilla in London Zoo.[185]

Lack of privacy in public spaces, caused by overcrowding, increases health issues in animals, including heart disease and high blood pressure. Also, the stress from overcrowding is connected to an increase in infant mortality rates and maternal stress. The lack of privacy that comes with overcrowding is connected to other issues in animals, which causes their relationships with others to diminish. How they present themselves to others of their species is a necessity in their life, and overcrowding causes the relationships to become disordered.[186]

For example, David Attenborough claims that the gorilla's right to privacy is being violated when they are looked at through glass enclosures. They are aware that they are being looked at, therefore they do not have control over how much the onlookers can see of them. Gorillas and other animals may be in the enclosures due to safety reasons, however Attenborough states that this is not an excuse for them to be constantly watched by unnecessary eyes. Also, animals will start hiding in unobserved spaces.[186] Animals in zoos have been found to exhibit harmful or different behaviours due to the presence of visitors watching them:[187]

- Cotton-top tamarins in zoos engage in less social behaviours, including physical contact and sex, than ones in off-exhibit buildings.
- Chimpanzees become more aggressive towards each other.
- Lion-tailed macaques pace and bite themselves more in direct proportions to human visitors.
- In one zoo, orangutans have been shown to cover their heads less as the density of visitors decreased.

See also

- Civil liberties

- Digital identity
- Global surveillance
- Identity theft in the United States
- Open data
- Open access
- Transparency
- Visual privacy
- Privacy software

References

1. Wells, John C. (2008). *Longman Pronunciation Dictionary* (3rd ed.). Longman. ISBN 978-1-4058-8118-0.
2. Jones, Daniel (2011). Roach, Peter; Setter, Jane; Esling, John (eds.). *Cambridge English Pronouncing Dictionary* (18th ed.). Cambridge University Press. ISBN 978-0-521-15255-6.
3. "privacy (n.)" (https://www.etymonline.com/word/privacy), *Etymology Dictionary*, November 17, 2020, retrieved November 18, 2020
4. Alibeigi, Ali; Munir, Abu Bakar; Karim, Md. Ershadul (2019). "Right to Privacy, A Complicated Concept to Review" (https://dx.doi.org/10.2139/ssrn.3537968). *SSRN Electronic Journal*. doi:10.2139/ssrn.3537968 (https://doi.org/10.2139%2Fssrn.3537968). ISSN 1556-5068 (https://search.worldcat.org/issn/1556-5068).
5. DeCew, Judith (2015), "Privacy" (https://plato.stanford.edu/archives/spr2015/entries/privacy/), in Zalta, Edward N.; Nodelman, Uri (eds.), *The Stanford Encyclopedia of Philosophy* (Spring 2015 ed.), Metaphysics Research Lab, Stanford University, retrieved 2024-03-21
6. "oremus Bible Browser : Ecclesiasticus 29:21" (https://bible.oremus.org/?passage=Ecclesiasticus%2029:21&version=nrsvae). *bible.oremus.org*. Retrieved 2024-03-21.
7. Konvitz, Milton R. (1966). "Privacy and the Law: A Philosophical Prelude" (https://www.jstor.org/stable/1190671). *Law and Contemporary Problems*. **31** (2): 272–280. doi:10.2307/1190671 (https://doi.org/10.2307%2F1190671). ISSN 0023-9186 (https://search.worldcat.org/issn/0023-9186). JSTOR 1190671 (https://www.jstor.org/stable/1190671).
8. Longfellow, Erica (2006). "Public, Private, and the Household in Early Seventeenth-Century England" (https://www.jstor.org/stable/10.1086/499790). *Journal of British Studies*. **45** (2): 313–334. doi:10.1086/499790 (https://doi.org/10.1086%2F499790). ISSN 0021-9371 (https://search.worldcat.org/issn/0021-9371). JSTOR 10.1086/499790 (https://www.jstor.org/stable/10.1086/499790).
9. Negley, Glenn (1966). "Philosophical Views on the Value of Privacy" (https://www.jstor.org/stable/1190674). *Law and Contemporary Problems*. **31** (2): 319–325. doi:10.2307/1190674 (https://doi.org/10.2307%2F1190674). ISSN 0023-9186 (https://search.worldcat.org/issn/0023-9186). JSTOR 1190674 (https://www.jstor.org/stable/1190674).
10. *Central Works of Philosophy: The Nineteenth Century* (https://www.jstor.org/stable/j.cttq4963). McGill-Queen's University Press. 2005. ISBN 978-0-7735-3052-2. JSTOR j.cttq4963 (https://www.jstor.org/stable/j.cttq4963).
11. Solove, Daniel J. (2006). "A Taxonomy of Privacy" (https://www.jstor.org/stable/40041279). *University of Pennsylvania Law Review*. **154** (3): 477–564. doi:10.2307/40041279 (https://doi.org/10.2307%2F40041279). ISSN 0041-9907 (https://search.worldcat.org/issn/0041-9907). JSTOR 40041279 (https://www.jstor.org/stable/40041279).
12. "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.
13. Information Privacy, Official Reference for the Certified Information privacy Professional (CIPP), Swire, 2007

14. "Nineteen Eighty-four | Summary, Characters, Analysis, & Facts" (https://www.britannica.com/topic/Nineteen-Eighty-four). *Encyclopedia Britannica*. Retrieved 2021-09-27.
15. Leetaru, Kalev. "As Orwell's 1984 Turns 70 It Predicted Much Of Today's Surveillance Society" (https://www.forbes.com/sites/kalevleetaru/2019/05/06/as-orwells-1984-turns-70-it-predicted-much-of-todays-surveillance-society/). *Forbes*. Retrieved 2021-09-27.
16. Solove 2010, pp. 3–4.
17. "Alan Westin is the father of modern data privacy law" (https://www.osano.com/articles/alan-westin). *Osano*. 2020-07-24. Retrieved 2021-09-28.
18. "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.com*. Bloomberg Businessweek. 2019-12-11. Retrieved 2021-06-02.
19. "United States v. Jones" (https://www.oyez.org/cases/2011/10-1259). *Oyez*. Retrieved 2021-09-27.
20. "Riley v. California" (https://www.oyez.org/cases/2013/13-132). *Oyez*. Retrieved 2021-09-27.
21. "Carpenter v. United States" (https://www.oyez.org/cases/2017/16-402). *Oyez*. Retrieved 2021-09-27.
22. "17 disturbing things Snowden has taught us (so far)" (https://www.pri.org/stories/2013-07-09/17-disturbing-things-snowden-has-taught-us-so-far). *The World from PRX*. 30 July 2016. Retrieved 2021-09-28.
23. "Privacy vs Security: A pointless false dichotomy?" (https://missinfogeek.net/privacy-vs-security-pt1/). Archived (https://web.archive.org/web/20230131000446/https://missinfogeek.net/privacy-vs-security-pt1/) from the original on 2023-01-31.
24. Ari Ezra Waldman (2021). "One Book in One Page". *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge University Press. p. x. doi:10.1017/9781108591386 (https://doi.org/10.1017%2F9781108591386). ISBN 978-1-108-49242-3.
25. "The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress" (https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress). April 2021. Archived (https://web.archive.org/web/20230422071359/https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress) from the original on 2023-04-22.
26. "The Web Means the End of Forgetting" (https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html). *The New York Times*. 2010-07-25. Archived (https://web.archive.org/web/20190310101907/https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html) from the original on 2019-03-10.
27. Cofone, Ignacio (2023). *The Privacy Fallacy: Harm and Power in the Information Economy* (https://www.cambridge.org/core/books/privacy-fallacy/547578F2A1AE0C40963105CE066B412E). New York: Cambridge University Press. ISBN 9781108995443.
28. Cofone, Ignacio (2023). *The Privacy Fallacy: Harm and Power in the Information Economy* (https://www.cambridge.org/core/books/privacy-fallacy/547578F2A1AE0C40963105CE066B412E). New York: Cambridge University Press. ISBN 9781108995443.
29. "Privacy" (https://www.eff.org/issues/privacy). *Electronic Frontier Foundation*.
30. "Legislative Reform" (https://cybercivilrights.org/legislative-reform/). *Cyber Civil Rights Initiative*.
31. Ben Tarnoff (2022). "Preface: Among the Eels". *Internet for the People: The Fight for Our Digital Future*. Verso Books. pp. 8–9. ISBN 978-1-83976-202-4.
32. "Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business" (https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business). *Federal Trade Commission*. 2013-05-02. Retrieved 2021-09-28.

33. Tiku, Nitasha. "How Europe's New Privacy Law Will Change the Web, and More" (https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Retrieved 2021-10-26.
34. "Children's Online Privacy Protection Rule ("COPPA")" (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule). *Federal Trade Commission*. 2013-07-25. Retrieved 2021-09-28.
35. "Fair Credit Reporting Act" (https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act). *Federal Trade Commission*. 19 July 2013. Retrieved 2023-06-18.
36. "Facebook: active users worldwide" (https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/). *Statista*. Retrieved 2020-10-11.
37. 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 Archived (https://web.archive.org/web/20140328144007/http://www.emeraldinsight.com/journals.htm?issn=1066-2243&volume=21&issue=4&articleid=1926600&show=abstract) 2014-03-28 at the Wayback Machine
38. 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): 5802–5805. 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).
39. "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.
40. Giroux, Henry A. (2015-05-04). "Selfie Culture in the Age of Corporate and State Surveillance". *Third Text*. **29** (3): 155–164. doi:10.1080/09528822.2015.1082339 (https://doi.org/10.1080%2F09528822.2015.1082339). ISSN 0952-8822 (https://search.worldcat.org/issn/0952-8822). S2CID 146571563 (https://api.semanticscholar.org/CorpusID:146571563).
41. 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://search.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).
42. CTVNews.ca Staff (October 14, 2012). "In wake of Amanda Todd suicide, MPs to debate anti-bullying motion" (http://www.ctvnews.ca/canada/in-wake-of-amanda-todd-suicide-mps-to-debate-anti-bullying-motion-1.995254). CTV News. Archived (https://web.archive.org/web/20131029213910/http://www.ctvnews.ca/canada/in-wake-of-amanda-todd-suicide-mps-to-debate-anti-bullying-motion-1.995254) from the original on October 29, 2013. Retrieved October 17, 2012.
43. Boutilier, Alex (April 13, 2014). "Amanda Todd's mother raises concerns about cyberbullying bill: Families of cyberbullying victims want legislation, but some have concerns about warrantless access to Canadians personal data" (https://www.thestar.com/news/canada/2014/05/13/amanda_todds_mother_raises_concerns_about_cyberbullying_bill.html). *www.thestar.com*. Archived (https://web.archive.org/web/20161028011059/https://www.thestar.com/news/canada/2014/05/13/amanda_todds_mother_raises_concerns_about_cyberbullying_bill.html) from the original on October 28, 2016. Retrieved September 12, 2016.
44. Todd, Carol (May 14, 2014). "Carol Todd's Testimony regarding Bill C-13" (https://openparliament.ca/committees/justice/41-2/24/carol-todd-1/). www.openparliament.ca. Archived (https://web.archive.org/web/20160918140017/https://openparliament.ca/committees/justice/41-2/24/carol-todd-1/) from the original on September 18, 2016. Retrieved September 12, 2016.

45. "Real-Name Online Registration to Be Scrapped" (https://english.chosun.com/site/data/html_dir/2011/12/30/2011123001526.html). *The Chosun Ilbo*. Archived (https://web.archive.org/web/20230423035426/https://english.chosun.com/site/data/html_dir/2011/12/30/2011123001526.html) from the original on 2023-04-23.
46. *Empirical analysis of online anonymity and user behaviors: the impact of real name policy* (https://www.computer.org/csdl/proceedings-article/hicss/2012/06149194/12OmNyKJiDq). Hawaii International Conference on System Sciences (45th ed.). IEEE Computer Society. 2012.
47. "Law, Policies and Regulations" (https://www.stopbullying.gov/resources/laws). 24 September 2019. Retrieved 2023-06-19.
48. "Florida Anti-Bullying Laws and Policies" (https://www.stopbullying.gov/resources/laws/florida). 24 September 2019. Retrieved 2023-06-19.
49. 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).
50. 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
51. Whittaker, Zack (Aug 22, 2017). "AccuWeather caught sending user location data – even when location sharing is off" (https://www.zdnet.com/article/accuweather-caught-sending-geo-location-data-even-when-denied-access/). *ZDNet*. Retrieved 2021-11-22.
52. Kirk, Jeremy (March 20, 2017). "McShame: McDonald's API Leaks Data for 2.2 Million Users" (https://www.bankinfosecurity.com/blogs/mcshame-mcdonalds-api-leaks-data-for-22-million-users-p-2426). *BankInfoSecurity*. Retrieved 2021-11-22.
53. Popkin, Helen A.S., "Government 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, "Technolog", April 21, 2011
54. Keizer, Gregg (2011-04-21). "Apple faces questions from Congress about iPhone tracking" (https://www.computerworld.com/article/2507868/apple-faces-questions-from-congress-about-iphone-tracking.html). *Computerworld*. Archived (https://web.archive.org/web/20190720044451/https://www.computerworld.com/article/2507868/apple-faces-questions-from-congress-about-iphone-tracking.html) from the original on 2019-07-20.
55. Keizer, Gregg (2011-04-27). "Apple denies tracking iPhone users, but promises changes" (https://www.computerworld.com/article/2506250/apple-denies-tracking-iphone-users--but-promises-changes.html). *Computerworld*. Archived (https://web.archive.org/web/20230329094239/https://www.computerworld.com/article/2506250/apple-denies-tracking-iphone-users--but-promises-changes.html) from the original on 2023-03-29.
56. "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.
57. "Global Digital Ad Spending 2019" (https://www.insiderintelligence.com/content/global-digital-ad-spending-2019). *Insider Intelligence*. Retrieved 2023-09-30.
58. Chen, Brian X. (2021-09-16). "The Battle for Digital Privacy Is Reshaping the Internet" (https://www.nytimes.com/2021/09/16/technology/digital-privacy.html). *The New York Times*. ISSN 0362-4331 (https://search.worldcat.org/issn/0362-4331). Retrieved 2021-11-22.

59. Hausfeld (2024-05-16). "Privacy by default, abuse by design: EU competition concerns about Apple's new app tracking policy" (https://www.hausfeld.com/de-de/was-wir-denken/competition-bulletin/privacy-by-default-abuse-by-design-eu-competition-concerns-about-apple-s-new-app-tracking-policy/). *Hausfeld* (in German). Retrieved 2024-06-28.
60. "Google Facing Fresh E.U. Inquiry Over Ad Technology" (https://www.nytimes.com/2021/06/22/business/google-antitrust-european-union.html). *The New York Times*. 2021-06-22. Archived (https://web.archive.org/web/20230415083901/https://www.nytimes.com/2021/06/22/business/google-antitrust-european-union.html) from the original on 2023-04-15.
61. "EFF technologist cites Google "breach of trust" on FLoC; key ad-tech change agent departs IAB Tech Lab" (https://itega.org/2021/04/02/privacy-beat-eff-technologist-cites-google-breach-of-trust-on-floc-key-ad-tech-change-agent-departs-iab-tech-lab/). *Information Trust Exchange Governing Association*. Retrieved April 16, 2021.
62. "Google's FLoC Is a Terrible Idea" (https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea). *Electronic Frontier Foundation*. 2021-03-03.
63. 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): 5802–5805. 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).
64. "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.
65. Solove 2010, p. 3.
66. Quinn, Michael J. (2009). *Ethics for the Information Age*. Pearson Addison Wesley. ISBN 978-0-321-53685-3.
67. "Privacy Guidelines" (http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm). OECD. Retrieved 2019-08-22.
68. Cate, Fred H.; Collen, Peter; Mayer-Schönberger, Viktor. Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines (https://web.archive.org/web/20181231160753/https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf) (PDF) (Report). Archived from the original (https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf) (PDF) on 2018-12-31. Retrieved 2019-02-01.
69. Jensen, Carlos (2004). *Privacy policies as decision-making tools: an evaluation of online privacy notices*. CHI (http://www.chi2004.org/index.html).
70. "The Privacy Act" (https://www.oaic.gov.au/privacy/the-privacy-act). *Home*. 10 March 2023.
71. "For Your Information" (http://www.alrc.gov.au/publications/report-108). Alrc.gov.au. 2008-08-12. Retrieved 2019-08-22.
72. Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (https://www.comlaw.gov.au/Details/C2012A00197).
73. Branch, Legislative Services (2023-09-01). "Consolidated federal laws of Canada, Privacy Act" (https://laws-lois.justice.gc.ca/eng/ACTS/P-21/page-1.html). *laws-lois.justice.gc.ca*. Retrieved 2024-03-21.
74. Power, Michael (2020). *Access to Information and Privacy*. LexisNexis Canada Inc. pp. HAP-51.
75. Branch, Legislative Services (2019-06-21). "Consolidated federal laws of Canada, Personal Information Protection and Electronic Documents Act" (https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html). *laws-lois.justice.gc.ca*. Retrieved 2024-03-21.

76. Power, Michael (2020). *Access to Information and Privacy*. LexisNexis Canada Inc. pp. HAP-81.
77. Cofone, Ignacio (2020). "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence" (https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/). Office of the Privacy Commissioner.
78. Cofone, Ignacio (2021). *Class Actions in Privacy Law*. Routledge.
79. Jones v. Tsige, 2012 ONCA 32 (CanLII), online: https://canlii.ca/t/fpnld.
80. Branch, Legislative Services (2020-08-07). "Consolidated federal laws of Canada, THE CONSTITUTION ACTS, 1867 to 1982" (https://laws-lois.justice.gc.ca/eng/const/page-12.html). *laws-lois.justice.gc.ca*. Retrieved 2024-03-22.
81. Penney, Steven; Rondinelli, Vincenzo; James, Stribopoulos (2013). *Criminal Procedure in Canada*. LexisNexis Canada Inc. pp. 143–77.
82. "- Civil Code of Québec" (https://www.legisquebec.gouv.qc.ca/en/document/cs/ccq-1991/20170616#:~:text=Every%20person%20has%20a%20right,64,%20a.). *www.legisquebec.gouv.qc.ca*. Retrieved 2024-03-22.
83. "- Charter of human rights and freedoms" (https://www.legisquebec.gouv.qc.ca/en/document/cs/c-12). *www.legisquebec.gouv.qc.ca*. Retrieved 2024-03-22.
84. Zhong, Guorong (2019). "E-Commerce Consumer Privacy Protection Based on Differential Privacy" (https://doi.org/10.1088%2F1742-6596%2F1168%2F3%2F032084). *Journal of Physics: Conference Series*. **1168** (3): 032084. Bibcode:2019JPhCS1168c2084Z (https://ui.adsabs.harvard.edu/abs/2019JPhCS1168c2084Z). doi:10.1088/1742-6596/1168/3/032084 (https://doi.org/10.1088%2F1742-6596%2F1168%2F3%2F032084). S2CID 169731837 (https://api.semanticscholar.org/CorpusID:169731837).
85. 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.
86. 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.
87. "What Happens When a Billion Identities Are Digitized?" (https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized). *Yale Insights*. 27 March 2020. Retrieved 2021-11-22.
88. 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).
89. McCarthy, Julie (2017-08-24). "Indian Supreme Court Declares Privacy A Fundamental Right" (https://www.npr.org/sections/thetwo-way/2017/08/24/545963181/indian-supreme-court-declares-privacy-a-fundamental-right). *NPR*. Retrieved 2021-11-22.
90. Saberin, Zeenat. "India's top court upholds validity of biometric ID card" (https://www.aljazeera.com/news/2018/9/26/indias-top-court-upholds-constitution-validity-of-aadhaar-card). *www.aljazeera.com*. Retrieved 2021-11-22.
91. Does Beckham judgment change rules? (http://news.bbc.co.uk/1/hi/uk/4482073.stm), from BBC News (retrieved 27 April 2005).
92. "Personal Information Toolkit" (http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/toolkit.pdf) Archived (https://web.archive.org/web/20090103165639/http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/toolkit.pdf) 2009-01-03 at the Wayback Machine Information Commissioner's Office, UK
93. DeCew, Judith (2015-01-01). Zalta, Edward N. (ed.). *Privacy* (http://plato.stanford.edu/archives/spr2015/entries/privacy/) (Spring 2015 ed.). Metaphysics Research Lab, Stanford University.

94. "Fourth Amendment" (https://www.law.cornell.edu/wex/fourth_amendment). *LII / Legal Information Institute*. Retrieved 2021-03-20.
95. "DOBBS v. JACKSON WOMEN'S HEALTH ORGANIZATION" (https://www.law.cornell.edu/supremecourt/text/19-1392). *LII / Legal Information Institute*. Retrieved 2022-06-25.
96. Frias, Lauren. "What is Griswold v. Connecticut? How access to contraception and other privacy rights could be at risk after SCOTUS overturned Roe v. Wade" (https://www.businessinsider.com/contraception-access-privacy-rights-at-risk-overturned-roe-v-wade-2022-6). *Business Insider*. Retrieved 2022-06-25.
97. "The Privacy Act" (https://web.archive.org/web/20150810064120/https://foia.state.gov/Learn/PrivacyAct.aspx). *Freedom of Information Act*. US Department of State. 2015-05-22. Archived from the original (https://foia.state.gov/Learn/PrivacyAct.aspx) on 2015-08-10. Retrieved 2015-11-19.
98. Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq.
99. Fourth Amendment to the United States Constitution
100. "Visit to the United States of America" (https://undocs.org/A/HRC/46/37/Add.4).
101. Nissenbaum, Helen (2009). *Privacy in Context Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press. ISBN 978-0804772891.
102. Solove 2010, pp. 15–17.
103. Warren and Brandeis, "The Right To Privacy" (http://www.law.louisville.edu/library/collections/brandeis/node/225)(1890) 4 Harvard Law Review 193
104. Solove 2010, p. 19.
105. 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): 729–739.
106. 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): 633–638. doi:10.1089/cyber.2013.0585 (https://doi.org/10.1089%2Fcyber.2013.0585). PMID 25226054 (https://pubmed.ncbi.nlm.nih.gov/25226054).
107. Gavison, Ruth (1980). "Privacy and the Limits of Law". *Yale Law Journal*. **89** (3): 421–471. doi:10.2307/795891 (https://doi.org/10.2307%2F795891). JSTOR 795891 (https://www.jstor.org/stable/795891).
108. 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.
109. Solove 2010, p. 24.
110. 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.
111. "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.
112. Mantelero, Alessandro (2014-12-01). "The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics" (https://www.sciencedirect.com/science/article/abs/pii/S026736491400154X). *Computer Law & Security Review*. **30** (6): 643–660. doi:10.1016/j.clsr.2014.09.004 (https://doi.org/10.1016%2Fj.clsr.2014.09.004). ISSN 0267-3649 (https://search.worldcat.org/issn/0267-3649). S2CID 61135032 (https://api.semanticscholar.org/CorpusID:61135032).
113. Westin, Alan (1967). *Privacy and Freedom*. New York: Atheneum.

114. Hughes, Kirsty (2012). "A Behavioural Understanding of Privacy and Its Implications for Privacy Law". *The Modern Law Review*. **75** (5): 806–836. doi:10.1111/j.1468-2230.2012.00925.x (https://doi.org/10.1111%2Fj.1468-2230.2012.00925.x). S2CID 142188960 (https://api.semanticscholar.org/CorpusID:142188960).
115. Johnson, Carl A. (1974). "Privacy as Personal Control" (https://www.researchgate.net/publication/268370076). *Man-environment Interactions: Evaluations and Applications: Part 2*. **6**: 83–100.
116. Johnson 1974, p. 90.
117. Johnson 1974, pp. 85–89.
118. Magnani, Lorenzo (2007). "4, "Knowledge as Duty: Cyberprivacy" ". *Morality in a Technological World: Knowledge as Duty*. Cambridge: Cambridge University Press. pp. 110–118. doi:10.1017/CBO9780511498657 (https://doi.org/10.1017%2FCBO9780511498657). ISBN 9780511498657.
119. Magnani (2007), p. 116, ch. 4, "Knowledge as Duty: Cyberprivacy".
120. Johnson 1974, pp. 90–92.
121. Solove 2010, p. 21.
122. 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.
123. Solove 2010, pp. 22–23.
124. Reiman, Jeffrey (1976). "Privacy, Intimacy, and Personhood". *Philosophy & Public Affairs*.
125. Benn, Stanley. "Privacy, freedom, and respect for persons". In Schoeman, Ferdinand (ed.). *Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press.
126. Kufer, Joseph (1987). "Privacy, Autonomy, and Self-Concept". *American Philosophical Quarterly*.
127. Goffman, Erving (1968). *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. New York: Doubleday.
128. Altman, Irwin (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey: Brooks/Cole Publishing Company.
129. Solove 2010, p. 35.
130. Rachels, James (Summer 1975). "Why Privacy is Important". *Philosophy & Public Affairs*. **4** (4): 323–333. JSTOR 2265077 (https://www.jstor.org/stable/2265077).
131. Citron, Danielle (2019). "Sexual Privacy" (https://scholarship.law.bu.edu/faculty_scholarship/620/). *Yale Law Journal*. **128**: 1877, 1880.
132. H. Jeff Smith (1994). *Managing Privacy: Information Technology and Corporate America* (https://archive.org/details/managingprivacyi0000smit). UNC Press Books. ISBN 978-0807821473.
133. "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.
134. "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.
135. "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.
136. Popa, C., et al., "Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy-Savvy Leaders", Carswell (2012), Ch. 6

137. 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.
138. Posner, R. A. (1981). "The economics of privacy". *The American Economic Review*. **71** (2): 405–409.
139. Lessig (2006), p. 229: "In my view, the protection of privacy would be stronger if people conceived of the right as a property right.".
140. Lessig (2006).
141. Johnson, Deborah (2009). Beauchamp; Bowie; Arnold (eds.). *Ethical theory and business* (8th ed.). Upper Saddle River, NJ: Pearson/Prentice Hall. pp. 428–442. ISBN 978-0-13-612602-7.
142. Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill: The University of North Carolina Press.
143. "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.
144. Shade, L.R. (2008). "Reconsidering the right to privacy in Canada". *Bulletin of Science, Technology & Society*, 28(1), 80–91.
145. Watt, Eliza. "The role of international human rights law in the protection of online privacy in the age of surveillance." (http://eprints.bournemouth.ac.uk/30324/1/THE%20ROLE%20OF%20INTERNATIONAL%20LAW%20AND%20CYBER%20SURVEILLANCE-CYCON%20TALLIN%202017.pdf) In 2017 9th International Conference on Cyber Conflict (CyCon), pp. 1–14. IEEE, 2017.
146. Swartz, J., "'Opting In': A Privacy Paradox", The Washington Post, 03 Sep 2000, H.1.
147. 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.
148. J. Sweat "Privacy paradox: Customers want control – and coupons", *Information Week*, Manhasset Iss, 781, April 10, 2000, p. 52.
149. "Volume 11, Number 9" (https://firstmonday.org/ojs/index.php/fm/issue/view/203). *firstmonday.org*. 4 September 2006. Retrieved 2019-11-25.
150. Taddicken, Monika (January 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): 248–273. doi:10.1111/jcc4.12052 (https://doi.org/10.1111%2Fjcc4.12052).
151. Nemec Zlatolas, Lili; Welzer, Tatjana; Heričko, Marjan; Hölbl, Marko (April 2015). "Privacy antecedents for SNS self-disclosure: The case of Facebook" (https://linkinghub.elsevier.com/retrieve/pii/S0747563214007274). *Computers in Human Behavior*. **45**: 158–167. doi:10.1016/j.chb.2014.12.012 (https://doi.org/10.1016%2Fj.chb.2014.12.012).
152. Baruh, Lemi; Secinti, Ekin; Cemalcilar, Zeynep (February 2017). "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis" (https://academic.oup.com/joc/article/67/1/26-53/4082433). *Journal of Communication*. **67** (1): 26–53. doi:10.1111/jcom.12276 (https://doi.org/10.1111%2Fjcom.12276).
153. Gerber, Nina; Gerber, Paul; Volkamer, Melanie (August 2018). "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior" (https://linkinghub.elsevier.com/retrieve/pii/S0167404818303031). *Computers & Security*. **77**: 226–261. doi:10.1016/j.cose.2018.04.002 (https://doi.org/10.1016%2Fj.cose.2018.04.002). S2CID 52884338 (https://api.semanticscholar.org/CorpusID:52884338).

154. Kaiser, Florian G.; Byrka, Katarzyna; Hartig, Terry (November 2010). "Reviving Campbell's Paradigm for Attitude Research" (http://journals.sagepub.com/doi/10.1177/1088868310366452). *Personality and Social Psychology Review*. **14** (4): 351–367. doi:10.1177/1088868310366452 (https://doi.org/10.1177%2F1088868310366452). ISSN 1088-8683 (https://search.worldcat.org/issn/1088-8683). PMID 20435803 (https://pubmed.ncbi.nlm.nih.gov/20435803). S2CID 5394359 (https://api.semanticscholar.org/CorpusID:5394359).
155. 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.
156. Cofone, Ignacio (2023). *The Privacy Fallacy: Harm and Power in the Information Economy* (https://www.cambridge.org/core/books/privacy-fallacy/547578F2A1AE0C40963105CE066B412E). New York: Cambridge University Press. ISBN 9781108995443.
157. 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).
158. 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. [1] (http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1) Archived (https://web.archive.org/web/20160413214515/http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1) 2016-04-13 at the Wayback Machine
159. 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): 1038–1058. doi:10.1016/j.tele.2017.04.013 (https://doi.org/10.1016%2Fj.tele.2017.04.013). ISSN 0736-5853 (https://search.worldcat.org/issn/0736-5853).
160. Kokolakis, Spyros (January 2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". *Computers & Security*. **64**: 122–134. doi:10.1016/j.cose.2015.07.002 (https://doi.org/10.1016%2Fj.cose.2015.07.002). S2CID 422308 (https://api.semanticscholar.org/CorpusID:422308).
161. 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://search.worldcat.org/issn/0736-5853).
162. Frik, Alisa; Gaudeul, Alexia (2020-03-27). "A measure of the implicit value of privacy under risk". *Journal of Consumer Marketing*. **37** (4): 457–472. doi:10.1108/JCM-06-2019-3286 (https://doi.org/10.1108%2FJCM-06-2019-3286). ISSN 0736-3761 (https://search.worldcat.org/issn/0736-3761). S2CID 216265480 (https://api.semanticscholar.org/CorpusID:216265480).
163. 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.
164. 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. 211–236, 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, S2CID 11701552 (https://api.semanticscholar.org/CorpusID:11701552)

165. Belliger, Andréa; Krieger, David J. (2018), "2. The Privacy Paradox", *Network Publicy Governance*, Digitale Gesellschaft, vol. 20, transcript Verlag, pp. 45–76, doi:10.14361/9783839442135-003 (https://doi.org/10.14361%2F9783839442135-003), ISBN 978-3-8394-4213-5, S2CID 239333913 (https://api.semanticscholar.org/CorpusID:239333913)
166. Laufer, Robert S.; Wolfe, Maxine (July 1977). "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory" (https://onlinelibrary.wiley.com/doi/10.1111/j.1540-4560.1977.tb01880.x). *Journal of Social Issues*. **33** (3): 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x (https://doi.org/10.1111%2Fj.1540-4560.1977.tb01880.x).
167. Culnan, Mary J.; Armstrong, Pamela K. (February 1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation" (http://pubsonline.informs.org/doi/abs/10.1287/orsc.10.1.104). *Organization Science*. **10** (1): 104–115. doi:10.1287/orsc.10.1.104 (https://doi.org/10.1287%2Forsc.10.1.104). ISSN 1047-7039 (https://search.worldcat.org/issn/1047-7039). S2CID 54041604 (https://api.semanticscholar.org/CorpusID:54041604).
168. Trepte, Sabine; Reinecke, Leonard; Ellison, Nicole B.; Quiring, Oliver; Yao, Mike Z.; Ziegele, Marc (January 2017). "A Cross-Cultural Perspective on the Privacy Calculus" (https://doi.org/10.1177%2F2056305116688035). *Social Media + Society*. **3** (1): 205630511668803. doi:10.1177/2056305116688035 (https://doi.org/10.1177%2F2056305116688035). ISSN 2056-3051 (https://search.worldcat.org/issn/2056-3051).
169. Krasnova, Hanna; Spiekermann, Sarah; Koroleva, Ksenia; Hildebrand, Thomas (June 2010). "Online Social Networks: Why We Disclose" (http://journals.sagepub.com/doi/10.1057/jit.2010.6). *Journal of Information Technology*. **25** (2): 109–125. doi:10.1057/jit.2010.6 (https://doi.org/10.1057%2Fjit.2010.6). ISSN 0268-3962 (https://search.worldcat.org/issn/0268-3962). S2CID 33649999 (https://api.semanticscholar.org/CorpusID:33649999).
170. Solove 2010, p. 101.
171. 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).
172. Solove 2010, p. 103.
173. 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): 617–639. doi:10.1177/0022243720920256 (https://doi.org/10.1177%2F0022243720920256). ISSN 0022-2437 (https://search.worldcat.org/issn/0022-2437). S2CID 218917353 (https://api.semanticscholar.org/CorpusID:218917353).
174. Esteve, Asunción (2017). "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA" (https://academic.oup.com/idpl/article-abstract/7/1/36/3097625?redirectedFrom=fulltext&login=false). *International Data Privacy Law*. **7** (1): 36–47. doi:10.1093/idpl/ipw026 (https://doi.org/10.1093%2Fidpl%2Fipw026).
175. Solove 2010, pp. 104–05.
176. "How to Encrypt Email (Gmail, Outlook, iOS, Yahoo, Android, AOL)" (https://www.pandasecurity.com/en/mediacenter/panda-security/how-to-encrypt-email/). *Panda Security Mediacenter*. 2021-03-02. Retrieved 2021-11-22.
177. "Signal Messenger: Speak Freely" (https://signal.org/en/index.html). *Signal Messenger*. Retrieved 2021-11-22.
178. Lee, Micah (2015-11-12). "Edward Snowden Explains How To Reclaim Your Privacy" (https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/). *The Intercept*. Retrieved 2024-01-29.
179. Cheng, Evelyn (2017-08-29). "Dark web finds bitcoin increasingly more of a problem than a help, tries other digital currencies" (https://www.cnbc.com/2017/08/29/dark-web-finds-bitcoin-increasingly-more-of-a-problem-than-a-help-tries-other-digital-currencies.html). *CNBC*. Retrieved 2024-01-29.

180. Ell, Kellie (2018-07-13). "Coinbase considers adding five new coins to its platform" (https://www.cnbc.com/2018/07/13/coinbase-considers-five-new-coins-for-its-platform.html). *CNBC*. Retrieved 2024-01-29.
181. "Anonymizers vs. VPNs: Everything You Need to Know" (https://blog.orchid.com/anonymizers-vs-vpns-everything-you-need-to-know/). *Privacy & VPN Blog – Orchid*. 2021-05-11. Retrieved 2022-01-22.
182. "7 Tips to Manage Your Identity and Protect Your Privacy Online" (https://staysafeonline.org/blog/7-tips-to-manage-your-identity/). *Stay Safe Online*. Retrieved 2021-11-22.
183. Gordon, Whitson (25 January 2019). "How to Protect Your Digital Privacy" (https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy). *The New York Times*. Retrieved 2021-11-22.
184. "Your Technology Is Tracking You. Take These Steps For Better Online Privacy : Life Kit" (https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy). *NPR.org*. Retrieved 2021-11-22.
185. "David Attenborough: zoos should use peepholes to respect gorillas' privacy" (https://www.theguardian.com/world/2016/oct/18/david-attenborough-zoos-respect-gorillas-privacy-peepholes). *The Guardian*. Agence France-Presse. 18 October 2016. Retrieved 10 August 2022.
186. Pepper, Angie (December 2020). "Glass Panels and Peepholes: Nonhuman Animals and the Right to Privacy" (https://onlinelibrary.wiley.com/doi/10.1111/papq.12329). *Pacific Philosophical Quarterly*. **101** (4): 628–650. doi:10.1111/papq.12329 (https://doi.org/10.1111%2Fpapq.12329). ISSN 0279-0750 (https://search.worldcat.org/issn/0279-0750).
187. Eveleth, Rose (31 January 2020). "Animals Need Digital Privacy Too" (https://www.wired.com/story/animals-need-digital-privacy-too/). *Wired*. Retrieved 10 August 2022.

Works cited

- Lessig, Lawrence (2006). "ELEVEN: Privacy". *Code* (https://archive.org/details/Code2.0/mode/2up) (2.0 ed.). Lawrence Lessig. ISBN 978-0-465-03914-2. Retrieved 30 June 2022.
- Solove, Daniel J. (2010). *Understanding Privacy*. Harvard University Press. ISBN 978-0674035072.

Further reading

- Singleton, Solveig (2008). "Privacy" (https://sk.sagepub.com/reference/libertarianism/n242.xml). In Hamowy, Ronald (ed.). *The Encyclopedia of Libertarianism* (https://books.google.com/books?id=yxNgXs3TkJYC). Thousand Oaks, CA: Sage; Cato Institute. pp. 390–392. doi:10.4135/9781412965811.n242 (https://doi.org/10.4135%2F9781412965811.n242). ISBN 978-1412965804. LCCN 2008009151 (https://lccn.loc.gov/2008009151). OCLC 750831024 (https://search.worldcat.org/oclc/750831024).

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*
- Wikipedia's privacy policy – Wikimedia Foundation