Information privacy

Information privacy is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.[1] It is also known as **data privacy**[2] or **data protection**.

Data privacy is challenging since it attempts to use data while protecting an individual's privacy preferences and personally identifiable information.[3] The fields of computer security, data security, and information security all design and use software, hardware, and human resources to address this issue.

Contents

Authorities

Laws

- General Data Protection Regulation (GDPR) (European Union)[4]
- General Personal Data Protection Law (Brazil)
- Data Protection Directive (European Union)
- California Consumer Privacy Act (CCPA) (California)
- Privacy Act (Canada)
- Privacy Act 1988 (Australia)

- Personal Data Protection Bill 2019 (India)
- China Cyber Security Law (CCSL) (China)
- Data Protection Act, 2012 (Ghana)
- Personal Data Protection Act 2012 (Singapore)[5]
- Republic Act No. 10173: Data Privacy Act of 2012 (Philippines)[6]
- Data protection (privacy) laws in Russia
- Data Protection Act 2018 (United Kingdom)
- Personal Data Protection Law (PDPL) (Bahrain)

Authorities by country

- National data protection authorities in the European Union and the European Free Trade Association
- Office of the Australian Information Commissioner (Australia)
- Privacy Commissioner (New Zealand)
- *Commission nationale de l'informatique et des libertés* (*CNIL*, France)
- Federal Commissioner for Data Protection and Freedom of Information (Germany)
- Office of the Privacy Commissioner for Personal Data (Hong Kong)
- Data Protection Commissioner (Ireland)
- Office of the Data Protection Supervisor (Isle of Man)
- National Privacy Commission (Philippines)
- Personal Data Protection Commission (Singapore)
- Personal Data Protection Office (Turkey) (KVKK, Turkey)
- Federal Data Protection and Information Commissioner (Switzerland)
- Information Commissioner's Office (ICO, United Kingdom)

Information types

Various types of personal information often come under privacy concerns.

Cable television

This describes the ability to control what information one reveals about oneself over cable television, and who can access that information. For example, third parties can track IP TV programs someone has watched at any given time. "The addition of any information in a broadcasting stream is not required for an audience rating survey, additional devices are not requested to be installed in the houses of viewers or listeners, and without the necessity of their cooperations, audience ratings can be automatically performed in real-time."[7]

Educational

In the United Kingdom in 2012, the Education Secretary Michael Gove described the National Pupil Database as a "rich dataset" whose value could be "maximised" by making it more openly accessible, including to private companies. Kelly Fiveash of *The Register* said that this could mean "a child's school life including exam results, attendance, teacher assessments and even characteristics" could be available, with third-party organizations being responsible for anonymizing any publications themselves, rather than the data being

anonymized by the government before being handed over. An example of a data request that Gove indicated had been rejected in the past, but might be possible under an improved version of privacy regulations, was for "analysis on sexual exploitation".[8]

Financial

Information about a person's financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases can be sensitive. If criminals gain access to information such as a person's accounts or credit card numbers, that person could become the victim of fraud or identity theft. Information about a person's purchases can reveal a great deal about that person's history, such as places he/she has visited, whom he/she has contacted with, products he/she has used, his/her activities and habits, or medications he/she has used. In some cases, corporations may use this information to target individuals with marketing customized towards those individual's personal preferences, which that person may or may not approve.[8]

Internet

The ability to control the information one reveals about oneself over the internet, and who can access that information, has become a growing concern. These concerns include whether email can be stored or read by third parties without consent, or whether third parties can continue to track the websites that someone visited. Another concern is if websites one visited can collect, store, and possibly share personally identifiable information about users.

The advent of various search engines and the use of data mining created a capability for data about individuals to be collected and combined from a wide variety of sources very easily.[9][10][11] The FTC has provided a set of guidelines that represent widely accepted concepts concerning fair information practices in an electronic marketplace called the Fair Information Practice Principles.

To avoid giving away too much personal information, emails should be encrypted. Browsing of web pages as well as other online activities should be done trace-less via "anonymizers", in case those are not trusted, by open-source distributed anonymizers, so called mix nets, such as I2P or Tor – The Onion Router. VPNs (Virtual Private Networks) are another "anonymizer" that can be used to give someone more protection while online. This includes obfuscating and encrypting web traffic so that other groups cannot see or mine it.[12]

Email isn't the only internet content with privacy concerns. In an age where increasing amounts of information is online, social networking sites pose additional privacy challenges. People may be tagged in photos or have valuable information exposed about themselves either by choice or unexpectedly by others, referred to as participatory surveillance. Data about location can also be accidentally published, for example, when someone posts a picture with a store as a background. Caution should be exercised when posting information online, social networks vary in what they allow users to make private and what remains publicly accessible.[13] Without strong security settings in place and careful attention to what remains public, a person can be profiled by searching for and collecting disparate pieces of information, worst case leading to cases of cyberstalking[14] or reputation damage.[15]

Cookies are used in websites that users may allow the website to retrieve some information from user's internet which it usually does not mention what the data being retrieved is.[16] It is a common method used to monitor and track users' internet activity.[16] In 2018, the General Data Protection Regulation (GDPR) passed regulation that forces websites to visibly disclose to consumers their information privacy practices, referred to as cookie notices.[17] This was issued to give consumers the choice of what information about their behavior they consent to letting websites track, however its effectiveness is controversial.[17] Some websites may

engage in deceptive practices such as placing the cookie notices in places on the page that are not visible, or only giving consumers notice that their information is being tracked, but not allowing them to change their privacy settings.[17]

Locational

As location tracking capabilities of mobile devices are advancing (location-based services), problems related to user privacy arise. Location data is among the most sensitive data currently being collected.[18] A list of potentially sensitive professional and personal information that could be inferred about an individual knowing only his mobility trace was published recently by the Electronic Frontier Foundation.[19] These include the movements of a competitor sales force, attendance of a particular church or an individual's presence in a motel, or at an abortion clinic. A recent MIT study[20][21] by de Montjoye et al. showed that four spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5 million people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity.

Medical

People may not wish for their medical records to be revealed to others due to the confidentiality and sensitivity of what the information could reveal about their health. For example, they might be concerned that it might affect their insurance coverage or employment. Or, it may be because they would not wish for others to know about any medical or psychological conditions or treatments that would bring embarrassment upon themselves. Revealing medical data could also reveal other details about one's personal life.[22] There are three major categories of medical privacy: informational (the degree of control over personal information), physical (the degree of physical inaccessibility to others), and psychological (the extent to which the doctor respects patients' cultural beliefs, inner thoughts, values, feelings, and religious practices and allows them to make personal decisions).[23] Physicians and psychiatrists in many cultures and countries have standards for doctor–patient relationships, which include maintaining confidentiality. In some cases, the physician–patient privilege is legally protected. These practices are in place to protect the dignity of patients, and to ensure that patients feel free to reveal complete and accurate information required for them to receive the correct treatment.[24] To view the United States' laws on governing privacy of private health information, see HIPAA and the HITECH Act. The Australian law is the Privacy Act 1988 Australia (https://www.legislation.gov.au/Details/C2020C00025) as well as state-based health records legislation.

Political

Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot is the simplest and most widespread measure to ensure that political views are not known to anyone other than the voters themselves—it is nearly universal in modern democracy, and considered to be a basic right of citizenship. In fact, even where other rights of privacy do not exist, this type of privacy very often does. Unfortunately, there are several forms of voting fraud or privacy violations possible with the use of digital voting machines.[25]

Legality

The legal protection of the right to privacy in general – and of data privacy in particular – varies greatly around the world.[26]

Laws and regulations related to Privacy and Data Protection are constantly changing, it is seen as important to keep abreast of any changes in the law and to continually reassess compliance with data privacy and security regulations.[27] Within academia, Institutional Review Boards function to assure that adequate measures are taken to ensure both the privacy and confidentiality of human subjects in research.[28]

Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Informed consent mechanisms including dynamic consent are important in communicating to data subjects the different uses of their personally identifiable information. Data privacy issues may arise in response to information from a wide range of sources, such as:[29]

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Privacy breach
- Location-based service and geolocation
- Web surfing behavior or user preferences using persistent cookies
- Academic research

Protection of privacy in information systems

As heterogeneous information systems with differing privacy rules are interconnected and information is shared, policy appliances will be required to reconcile, enforce, and monitor an increasing amount of privacy policy rules (and laws). There are two categories of technology to address privacy protection in commercial IT systems: communication and enforcement.

Policy communication

- P3P – The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

Policy enforcement

- XACML – The Extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL – The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

Protecting privacy on the internet

On the internet many users give away a lot of information about themselves: unencrypted e-mails can be read by the administrators of an e-mail server, if the connection is not encrypted (no HTTPS), and also the internet service provider and other parties sniffing the network traffic of that connection are able to know the contents. The same applies to any kind of traffic generated on the Internet, including web browsing, instant messaging,

and others. In order not to give away too much personal information, e-mails can be encrypted and browsing of webpages as well as other online activities can be done traceless via anonymizers, or by open source distributed anonymizers, so-called mix networks. Well-known open-source mix nets include I2P – The Anonymous Network and Tor.

Improving privacy through individualization

Computer privacy can be improved through individualization. Currently security messages are designed for the "average user", i.e. the same message for everyone. Researchers have posited that individualized messages and security "nudges", crafted based on users' individual differences and personality traits, can be used for further improvements for each person's compliance with computer security and privacy.[30]

United States Safe Harbor program and passenger name record issues

The United States Department of Commerce created the International Safe Harbor Privacy Principles certification program in response to the 1995 Directive on Data Protection (Directive 95/46/EC) of the European Commission.[31] Both the United States and the European Union officially state that they are committed to upholding information privacy of individuals, but the former has caused friction between the two by failing to meet the standards of the EU's stricter laws on personal data. The negotiation of the Safe Harbor program was, in part, to address this long-running issue.[32] Directive 95/46/EC declares in Chapter IV Article 25 that personal data may only be transferred from the countries in the European Economic Area to countries which provide adequate privacy protection. Historically, establishing adequacy required the creation of national laws broadly equivalent to those implemented by Directive 95/46/EU. Although there are exceptions to this blanket prohibition – for example where the disclosure to a country outside the EEA is made with the consent of the relevant individual (Article 26(1)(a)) – they are limited in practical scope. As a result, Article 25 created a legal risk to organisations which transfer personal data from Europe to the United States.

The program regulates the exchange of passenger name record information between the EU and the US. According to the EU directive, personal data may only be transferred to third countries if that country provides an adequate level of protection. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.

The European Commission has set up the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party". The Working Party gives advice about the level of protection in the European Union and third countries.[33]

The Working Party negotiated with U.S. representatives about the protection of personal data, the Safe Harbor Principles were the result. Notwithstanding that approval, the self-assessment approach of the Safe Harbor remains controversial with a number of European privacy regulators and commentators.[34]

The Safe Harbor program addresses this issue in the following way: rather than a blanket law imposed on all organisations in the United States, a voluntary program is enforced by the Federal Trade Commission. U.S. organisations which register with this program, having self-assessed their compliance with a number of standards, are "deemed adequate" for the purposes of Article 25. Personal information can be sent to such organisations from the EEA without the sender being in breach of Article 25 or its EU national equivalents. The Safe Harbor was approved as providing adequate protection for personal data, for the purposes of Article 25(6), by the European Commission on 26 July 2000.[35]

Under the Safe Harbor, adoptee organisations need to carefully consider their compliance with the *onward transfer obligations*, where personal data originating in the EU is transferred to the US Safe Harbor, and then onward to a third country. The alternative compliance approach of "binding corporate rules", recommended by

many EU privacy regulators, resolves this issue. In addition, any dispute arising in relation to the transfer of HR data to the US Safe Harbor must be heard by a panel of EU privacy regulators.[36]

In July 2007, a new, controversial,[37] Passenger Name Record agreement between the US and the EU was made.[38] A short time afterwards, the Bush administration gave exemption for the Department of Homeland Security, for the Arrival and Departure Information System (ADIS) and for the Automated Target System from the 1974 Privacy Act.[39]

In February 2008, Jonathan Faull, the head of the EU's Commission of Home Affairs, complained about the US bilateral policy concerning PNR.[40] The US had signed in February 2008 a memorandum of understanding (MOU) with the Czech Republic in exchange of a visa waiver scheme, without concerting before with Brussels.[37] The tensions between Washington and Brussels are mainly caused by a lesser level of data protection in the US, especially since foreigners do not benefit from the US Privacy Act of 1974. Other countries approached for bilateral MOU included the United Kingdom, Estonia, Germany and Greece.[41]

See also

- Data sovereignty
- Data localization
- Digital inheritance
- Digital self-determination
- ePrivacy Regulation
- Genetic privacy
- Pirate Party
- Privacy
- Privacy by design
- Privacy enhancing technologies
- Privacy law
- Privacy software
- Web literacy (privacy)

Computer science specific

- Authentication
- Data loss prevention software
- Data retention
- Data security
- Differential privacy

Organisations

- Confederation of European Data Protection Organisations
- Data Privacy Day (28 January)
- International Association of Privacy Professionals (headquartered in USA)
- Privacy International (headquartered in UK)

Scholars working in the field

- Adam Back

- Cynthia Dwork
- Ian Goldberg
- Khaled El Emam
- Lance Cottrell
- Latanya Sweeney
- Peter Gutmann
- Stefan Brands

References

1. *Uberveillance and the social implications of microchip implants : emerging technologies*. Michael, M. G., Michael, Katina, 1976-. Hershey, PA. 30 September 2013. ISBN 978-1466645820. OCLC 843857020 (https://www.worldcat.org/oclc/843857020).
2. Ian Austen (June 22, 2011). "Canadian Inquiry Finds Privacy Issues in Sale of Used Products at Staples" (https://bits.blogs.nytimes.com/2011/06/22/canadian-inquiry-finds-privacy-issues-in-sale-of-used-products-at-staples). *The New York Times*. Retrieved 2019-05-14.
3. Vicenç Torra (2017), "Introduction", *Data Privacy: Foundations, New Developments and the Big Data Challenge*, Studies in Big Data, **28**, Springer International Publishing, pp. 1–21, doi:10.1007/978-3-319-57358-8_1 (https://doi.org/10.1007%2F978-3-319-57358-8_1), ISBN 9783319573564
4. https://ec.europa.eu/info/law/law-topic/data-protection_en
5. https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview Retrieved 20 Oct 2019
6. Republic Act No. 10173: Data Privacy Act of 2012 (https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/)
7. "System for Gathering TV Audience Rating in Real Time in Internet Protocol Television Network and Method Thereof" (http://www.freepatentsonline.com/y2010/0011389.html). *FreePatentsOnline.com*. 2010-01-14. Retrieved 2011-06-07.
8. Fiveash, Kelly (2012-11-08). "Psst: Heard the one about the National Pupil Database? Thought not" (https://www.theregister.co.uk/2012/11/08/national_pupil_database_regulation_overhaul_in_private_sector_data_grab/). *The Register*. Retrieved 2012-12-12.
9. Bergstein, Brian (2006-06-18). "Research explores data mining, privacy" (https://www.usatoday.com/tech/news/surveillance/2006-06-18-data-mining-privacy_x.htm). *USA Today*. Retrieved 2010-05-05.
10. Bergstein, Brian (2004-01-01). "In this data-mining society, privacy advocates shudder" (http://www.seattlepi.com/business/154986_privacychallenge02.html). *Seattle Post-Intelligencer*.
11. Swartz, Nikki (2006). "U.S. Demands Google Web Data" (https://web.archive.org/web/20141219105358/http://connection.ebscohost.com/c/articles/21472572/u-s-demands-google-web-data). *Information Management Journal*. Archived from the original (http://connection.ebscohost.com/c/articles/21472572/u-s-demands-google-web-data) on 2014-12-19. Vol. 40 Issue 3, p. 18
12. "VyprVPN Protects Your Privacy and Security | Golden Frog" (https://www.vyprvpn.com/why-vpn/protect-privacy-and-security). *www.vyprvpn.com*. Retrieved 2019-04-03.
13. Schneider, G.; Evans, J.; Pinard, K.T. (2008). *The Internet: Illustrated Series* (https://books.google.com/books?id=E1fQdrzxAPoC&pg=PA17-IA137). Cengage Learning. p. 156. ISBN 9781423999386. Retrieved 9 May 2018.
14. Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family* (https://archive.org/details/cyberstalkinghar00boci/page/268). Greenwood Publishing Group. pp. 268 (https://archive.org/details/cyberstalkinghar00boci/page/268). ISBN 9780275981181.

15. Cannataci, J.A.; Zhao, B.; Vives, G.T.; et al. (2016). *Privacy, free expression and transparency: Redefining their new boundaries in the digital age* (https://books.google.com/books?id=tGC_DQAAQBAJ&pg=PA26). UNESCO. p. 26. ISBN 9789231001888. Retrieved 9 May 2018.
16. Bornschein, Rico; Schmidt, Lennard; Maier, Erik (2020-02-21). "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices" (https://doi.org/10.1177%2F0743915620902143). *Journal of Public Policy & Marketing*. **39** (2): 135–154. doi:10.1177/0743915620902143 (https://doi.org/10.1177%2F0743915620902143). ISSN 0743-9156 (https://www.worldcat.org/issn/0743-9156).
17. Bornschein, Rico; Schmidt, Lennard; Maier, Erik (April 2020). "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices" (http://journals.sagepub.com/doi/10.1177/0743915620902143). *Journal of Public Policy & Marketing*. **39** (2): 135–154. doi:10.1177/0743915620902143 (https://doi.org/10.1177%2F0743915620902143). ISSN 0743-9156 (https://www.worldcat.org/issn/0743-9156).
18. Ataei, M.; Kray, C. (2016). "Ephemerality Is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS" (https://books.google.com/books?id=_BdADQAAQBAJ&pg=PA360). *Progress in Location-Based Services 2016*. Springer. pp. 357–374. ISBN 9783319472898. Retrieved 9 May 2018.
19. Blumberg, A. Eckersley, P. "On locational privacy and how to avoid losing it forever" (https://www.eff.org/wp/locational-privacy). EFF.
20. 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).
21. Palmer, Jason (March 25, 2013). "Mobile location data 'present anonymity risk' " (https://www.bbc.co.uk/news/science-environment-21923360). *BBC News*. Retrieved 12 April 2013.
22. Aurelia, Nicholas-Donald; Francisco, Matus, Jesus; SeungEui, Ryu; M, Mahmood, Adam (1 June 2017). "The Economic Effect of Privacy Breach Announcements on Stocks: A Comprehensive Empirical Investigation" (http://aisel.aisnet.org/amcis2011_submissions/341/). *aisnet.org*.
23. Serenko, Natalia; Lida Fan (2013). "Patients' Perceptions of Privacy and Their Outcomes in Healthcare" (http://aserenko.com/IJBHR_Serenko_Fan.pdf) (PDF). *International Journal of Behavioural and Healthcare Research*. **4** (2): 101–122. doi:10.1504/IJBHR.2013.057359 (https://doi.org/10.1504%2FIJBHR.2013.057359).
24. "If a patient is below the age of 18-years does confidentiality still works or should doctor breach and inform the parents?15years girl went for... - eNotes" (http://www.enotes.com/everyday-law-encyclopedia/doctor-patient-confidentiality). *eNotes*.
25. Zetter, Kim (2018-02-21). "The Myth of the Hacker-Proof Voting Machine" (https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 2019-04-03.
26. Rakower, Lauren (2011). "Blurred Line: Zooming in on Google Street View and the Global Right to Privacy" (http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1082&context=bjil). *brooklynworks.brooklaw.edu*. Archived (https://web.archive.org/web/20171005101128/http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1082&context=bjil) from the original on 2017-10-05.

27. Robert Hasty, Dr Trevor W. Nagel and Mariam Subjally, *Data Protection Law in the USA.* (Advocates for International Development, August 2013.)"Archived copy" (https://web.archive.org/web/20150925093457/http://www.a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf) (PDF). Archived from the original (http://a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf) (PDF) on 2015-09-25. Retrieved 2013-10-14.
28. "Institutional Review Board - Guidebook, CHAPTER IV - CONSIDERATIONS OF RESEARCH DESIGN" (https://www.hhs.gov/ohrp/education-and-outreach/archived-materials/index.html). *www.hhs.gov*. October 5, 2017. Retrieved October 5, 2017.
29. *Programme Management Managing Multiple Projects Successfully*. Mittal, Prashant. Global India Pubns. 2009. ISBN 978-9380228204. OCLC 464584332 (https://www.worldcat.org/oclc/464584332).
30. "The Myth of the Average User: Improving Privacy and Security Systems through Individualization (NSPW '15) | BLUES" (https://blues.cs.berkeley.edu/blog/2015/08/26/the-myth-of-the-average-user-improving-privacy-and-security-systems-through-individualization-nspw-15/). *blues.cs.berkeley.edu*. Retrieved 2016-03-11.
31. "Protection of personal data" (https://web.archive.org/web/20060616181201/http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm). European Commission. Archived from the original (http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm) on 16 June 2006.
32. Weiss and Archick, Martin A. and Kristin (May 19, 2016). "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield". *Congressional Research Service*.
33. Center, Electronic Privacy Information. "EPIC - Article 29 Working Party" (https://epic.org/privacy/art29wp/#:~:text=The%20Working%20Party%20on%20the,Member%20States,%20the%20European%20Data). *epic.org*. Retrieved 2021-03-20.
34. "SEC (2004) 1323: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce" (https://web.archive.org/web/20060724173657/http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf) (PDF). European Commission. 20 October 2004. Archived from the original (http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf) (PDF) on 24 July 2006.
35. "2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce" (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML). *Official Journal of the European Union, L Series*. 25 August 2000. pp. 7–47 – via Eur-Lex.
36. "Q&A on the European Data Protection Authorities Panel foreseen by the Safe Harbour Decision" (https://web.archive.org/web/20060724174212/http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/information_safe_harbour_en.pdf) (PDF). European Commission. Archived from the original (http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/information_safe_harbour_en.pdf) (PDF) on 2006-07-24.
37. A divided Europe wants to protect its personal data wanted by the US (http://www.rue89.com/2008/03/04/a-divided-europe-wants-to-protect-its-personal-data-wanted-by-the-us), *Rue 89*, 4 March 2008 (in English)
38. https://web.archive.org/web/20120112021643/http://www.libertysecurity.org/article1591.html
39. Statewatch, US changes the privacy rules to exemption access to personal data (http://www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm) September 2007
40. Brussels attacks new US security demands (http://euobserver.com/9/25657), European Observer. See also Statewatch newsletter (http://www.statewatch.org/news/) February 2008
41. Statewatch, March 2008

Further reading

- Philip E. Agre; Marc Rotenberg (1998). *Technology and privacy: the new landscape* (https://archive.org/details/technologyprivac0000agre). MIT Press. ISBN 978-0-262-51101-8.

External links

International

- Factsheet on ECtHR case law on data protection (https://web.archive.org/web/20120111162553/http://www.echr.coe.int/NR/rdonlyres/4FCF8133-AD91-4F7B-86F0-A448429BC2CC/0/FICHES_Protection_des_données_EN.pdf)
- International Conference of Data Protection and Privacy Commissioners (https://web.archive.org/web/20190904150616/https://icdppc.org/)
- Biometrics Institute Privacy Charter (https://web.archive.org/web/20120418083909/http://www.biometricsinstitute.org/pages/privacy-biometrics.html)

Europe

- EU data protection page (http://ec.europa.eu/justice_home/fsj/privacy/)
- UNESCO Chair in Data Privacy (http://unescoprivacychair.urv.cat/)
- European Data Protection Supervisor (http://www.edps.europa.eu/EDPSWEB/)

Latin America

- Latin American Data Protection Law Review (https://web.archive.org/web/20130108061616/http://www.rlpdp.com/)

North America

- Privacy and Access Council of Canada (http://www.pacc-ccap.ca/)
- Laboratory for International Data Privacy (http://privacy.cs.cmu.edu/) at Carnegie Mellon University.
- Privacy Laws by State (http://www.epic.org/privacy/consumer/states.html)

Journals

- IEEE Security & Privacy magazine (http://www.computer.org/security/)
- Transactions on Data Privacy (http://www.tdp.cat/)
