Information privacy

Information privacy, or **data privacy** (or **data protection**), is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

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. Data privacy issues may arise in response to information from a wide range of sources, such as:

- 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

The challenge of data privacy is to utilize data while protecting individual's privacy preferences and their personally identifiable information. The fields of computer security, data security, and information security design and utilize software, hardware, and human resources to address this issue. Since the laws and regulations related to Privacy and Data Protection are constantly changing, it is important to keep abreast of any changes in the law and to continually reassess compliance with data privacy and security regulations.[1] Within academia, Institutional Review Boards function to assure that adequate measures are taken to insure both the privacy and confidentiality of human subjects in research[2].

Contents

Information types

Various types of personal information often come under privacy concerns.

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 has visited. Another concern is if the websites that are 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.[3][4][5] 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.

In order not to give away too much personal information, e-mails should be encrypted. Browsing of webpages 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.

Email isn't the only Internet use with concern of privacy. Everything is accessible over the Internet nowadays. However, a major issue with privacy relates back to social networking. For example, there are millions of users on Facebook and its regulations have changed. People may be tagged in photos or have valuable information exposed about themselves either by choice or, most of the time, unexpectedly by others. It is important to be cautious of what is being said over the Internet and what information is being displayed as well as photos because this all can be searched across the web and used to access private databases, making it easy for anyone to quickly go online and profile a person.

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 cooperation, audience ratings can be automatically performed in real-time."[6]

Medical

People may not wish for their medical records to be revealed to others. This may be because they have concern that it might affect their insurance coverages 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.[7] 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).[8] 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 will feel free to reveal complete and accurate information required for them to receive the correct treatment.[9] To view the United States' laws on governing privacy of private health information, see HIPAA and the HITECH Act.

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.

Locational

As location tracking capabilities of mobile devices are advancing (Location-based service), problems related to user privacy arise. Location data is among the most sensitive data currently being collected. 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.[10] 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[11][12] by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity.

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.

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".[13]

Legality

The legal protection of the right toprivacy in general – and of data privacy in particular – varies greatly around the world.[14]

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.[15] 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.

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.[16]

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 FTC. 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.[17]

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.[18]

In July 2007, a new, controversial,[19] Passenger Name Record agreement between the US and the EU was made.[20] 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.[21]

In February 2008, Jonathan Faull, the head of the EU's Commission of Home Affairs, complained about the US bilateral policy concerning PNR.[22] 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.[19] 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.[23]

Protecting 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 o 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 to further improve each person's compliance with computer security and privacy.[24]

Authorities

Laws

- General Data Protection Regulation (European Union)
- Data Protection Directive (European Union)
- Data Protection Act 1998 (United Kingdom)
- Data Protection Act, 2012 (Ghana)
- Data protection (privacy) laws in Russia
- Personal Data Protection Act 2012 (Singapore)[25]
- Privacy Act (Canada)

Authorities by country

- National data protection authorities in the European Union and the European Free Trade Association
- Office of the Australian Information Commissioner (Australia)
- *Commission nationale de l'informatique et des libertés* (France)
- Federal Commissioner for Data Protection and Freedom of Information (Germany)
- Data Protection Commissioner (Ireland)
- Office of the Data Protection Supervisor (Isle of Man)
- Federal Data Protection and Information Commissioner (Switzerland)
- Information Commissioner's Office (United Kingdom)
- Privacy Commissioner for Personal Data (Hong Kong)[26]

See also

- Privacy
- ePrivacy Regulation
- Data sovereignty
- Data localization
- Digital Inheritance
- Genetic privacy
- Privacy enhancing technologies
- Privacy software (example: I2P – The Anonymous Network)
- Web literacy (Privacy)

Computer science specific

- Authentication
- Data security
- Data retention
- Data Loss Prevention
- Differential privacy

Organisations

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

Scholars working in the field

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

References

1. 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.
2. "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.
3. 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.
4. Bergstein, Brian (2004-01-01). "In this data-mining society, privacy advocates shudder" (http://www.seattlepi.com/business/154986_privacychallenge02.html) *Seattle Post-Intelligencer*.
5. Swartz, Nikki (2006). "U.S. Demands Google Web Data" (http://connection.ebscohost.com/c/articles/21472572/u-s-demands-google-web-data) *Information Management Journal* Vol. 40 Issue 3, p. 18
6. "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.
7. 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*.
8. 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.
9. "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*.
10. Blumberg, A. Eckersley P. "On locational privacy and how to avoid losing it forever" (https://www.eff.org/wp/locational-privacy). EFF.
11. 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" (http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html). *Nature srep*. doi:10.1038/srep01376 (https://doi.org/10.1038%2Fsrep01376). Retrieved 12 April 2013.

12. Palmer, Jason (March 25, 2013). "Mobile location data 'present anonymity risk'" (http://www.bbc.co.uk/news/science-environment-21923360) *BBC News*. Retrieved 12 April 2013.
13. 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.
14. Rakower, Lauren (2011). "Blurred Line: Zooming in on Google Street View and the Global Right to Privacy" (http://brooklynworks.brooklaw.edu/bjil/vol37/iss1/8/) *http://brooklynworks.brooklaw.edu/*. Archived from the original (http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1082&context=bjil) on |archive-url= requires |archive-date= (help). External link in |website= (help)
15. "Protection of personal data – European Commission" (http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm). *ec.europa.eu*.
16. "Protection of personal data – European Commission" (http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf) (PDF). *ec.europa.eu*.
17. "EUR-Lex – 32000D0520 – EN" (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML). *eur-lex.europa.eu*.
18. "Protection of personal data – European Commission" (http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/information_safe_harbour_en.pdf) (PDF). *ec.europa.eu*.
19. 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)
20. http://www.libertysecurity.org/article1591.html
21. 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
22. Brussels attacks new US security demands (http://euobserver.com/9/25657), European Observer. See also Statewatch newsletter (http://www.statewatch.org/news/) February 2008
23. Statewatch, March 2008
24. "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.
25. "Personal Data Protection Act Overview" (https://www.pdpc.gov.sg/legislation-and-guidelines/overview) *www.pdpc.gov.sg*.
26. The Office of the Privacy Commissioner for Personal Data Website (https://www.pcpd.org.hk/english/about_pcpd/our_role/what_we_do.html)

Further reading

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

External links

International

- Factsheet on ECtHR case law on data protection
- International Conference of Data Protection and Privacy Commissioners
- Biometrics Institute Privacy Charter

Europe

- EU data protection page
- UNESCO Chair in Data Privacy
- European Data Protection Supervisor

Latin America

- Latin American Data Protection Law Review

North America

- Privacy and Access Council of Canada
- Laboratory for International Data Privacy at Carnegie Mellon University
- Privacy Laws by State

Journals

- IEEE Security & Privacy magazine
- Transactions on Data Privacy
