5-899 / 17-500 Usable Privacy and Security
Introduction to Privacy

Lecture by *Lorrie Cranor*
Scribe notes by *Ponnurangam K*
January 24, 2006

1 Topics covered

- What is Privacy?
- Privacy laws and self-regulation
- Privacy policies
- Platform for Privacy Preferences (P3P)
- Privacy risks from personalization

1.1 What is Privacy?

Privacy has many definitions and dimensions; there are different views about privacy. Dr. Alan Westin in his book *Privacy and Freedom* specifies privacy as

> ... the claim of individuals, groups or institutions [organizations] to determine for themselves when, how, and to what extent information about them is communicated to others... voluntary and temporary withdrawal of a person from the general society through physical or psychological means... anonymity or reserve...privacy is never absolute... he [individual] balances the desire for privacy with the desire for disclosure and communication [39, pp.7].

Along the same definition, Fred Cate defines privacy as

> ... Privacy is not an absolute. It is contextual and subjective... valuation [the consequences] will depend significantly on who [individual] is making it... neither privacy values nor costs are absolute...[17, pp. 199].

Other definitions of privacy are:

> ... right to be left alone [37].
>
> ... desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves [32].

So it is necessary to understand that the definition of privacy varies from individual to individual or organization to organization. It is also context specific. It is not necessary to accept one universal view for privacy in all situations.

Westin has created four states of privacy [38]:

1. **Solitude** is the state where the individual wants to be completely alone, out of the sight and hearing of anyone else. This state is the most complete and relaxed condition of privacy.

2. **Intimacy** is the state where individuals seek valued and trusted relationships with family, friends, or associates. The individual is part of a small unit.

3. **Anonymity** is the state in which individuals expect privacy being in public. This is the condition of being seen or heard but not known.

4. **Reserve** is the state where the individuals does not wish certain sensitive personal aspects to be discussed or noticed. In this state individuals hold back communication among others.

Westin also has created one or more Privacy Indexes to summarize his results and to show trends in privacy concerns among the American public [26]. He has classified public into the three categories [40]:

1. **Privacy Fundamentalists** are generally distrustful of organizations that ask for their personal information, worried about the accuracy of computerized information and additional uses made of it, and are in favor of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies. They generally choose privacy controls over consumer-service benefits when these compete with other. About 25% of the public are privacy fundamentalists.

2. **The Unconcerned** are generally trustful of organizations collecting their personal information, comfortable with existing organizational procedures and users are ready to forego privacy claims to secure consumer-service benefits or public-order values and not in favor of the enactment of new privacy laws or regulations. About 18% of public fall into this category.

3. **The Pragmatist** weigh the benefits to them of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved. They look to see what practical procedures for accuracy, challenge and correction of errors, business organization or government agency follows when consumer or citizen evaluations are involved. They believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it. And, where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists. About 57% of public fall into this category.

1.2 Privacy laws and self-regulation

1.2.1 Privacy laws

Privacy laws were created very recently; in specific, most of the laws related to privacy were written after 1970. The framework of privacy laws across the globe has been implemented in two different approaches. Europe has comprehensive or omnibus laws for data protection of the citizens, while US has implemented sector specific laws [27], [33]. Most of the other countries follow one of these approaches in implementing privacy laws. These two approaches have fundamental differences; and both approaches have respective advantages and disadvantages [33, chapter 2]. The essential purpose of these privacy laws is to protect the personal information of an individual or organization. Examples of laws in different countries are: US (HIPPA [36]; COPPA [1], [9]; GLB [31]), Europe (The European Privacy Directive [18]), Canada (Privacy Act [15]), Australia (Privacy Act 1988 [28]) and there are plans for a privacy law in India [16].

Organization for Economic Co-operation and Development (OECD) has created basic principles to protect personal information of an individual or organization in Europe. The guideline defines the *Data Controller* as "... a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body." And the *Data subject* is an individual who is the subject of a personal data record [29]. OECD has developed the following basic principles to protect the personal data of individuals [29]:

- **Collection Limitation Principle -** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle -** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle -** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use Limitation Principle -** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.

- **Security Safeguards Principle -** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- **Openness Principle -** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence

and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation Principle -** An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her.

- **Accountability Principle -** A data controller should be accountable for complying with measures which give effect to the principles stated above.

US organizations initially did not take the OECD guidelines seriously, but eventually US had to write simplified principles of OECD guidelines in order to conduct business with European countries. Federal Trade Commission (FTC) created the following simplified principles [19]:

- **Notice / Awareness -** Consumers should be given notice of an entity's information practices before any personal information is collected from them.

- **Choice / Consent -** Choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information

- **Access / Participation -** It refers to an individual's ability both to access data about him or herself i.e., to view the data in an entity's files and to contest that data's accuracy and completeness.

- **Integrity / Security -** Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.

- **Enforcement / Redress -** In absence of an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles.

1.2.2 Self-regulation

In the US, self-regulated programs were created to oversee the organizations while protecting the personal information of the users. One outcome of this

self-regulation is the formation of the seal programs. Privacy Seals Programs are the third-party organizations which help build confidence among consumers by authorizing the quality of the data protection in the organization. Few seal programs are:

- TRUSTe - http://www.truste.org
- BBBOnline - http://www.bbbonline.org
- CPA WebTrust - http://www.cpawebtrust.org/
- Japanese Privacy Mark - http://privacymark.org/

1.3 Privacy policies

Organizations are always looking for more customers and business. They increase business and customers in part by increasing credibility and trust among consumers [7], [20, pp. 148]. Studies have shown a direct relationship between trust and privacy [23], [41]. An organization can improve the credibility and trust among its customers by protecting consumers' privacy. Organizations express their privacy procedures for protecting the personal information of the consumers through privacy policies. Privacy policies represent the organization's privacy practices as privacy promises. In general, a "privacy policy" is defined as:

> what data is collected, for what purpose the data will be used, whether the enterprise provides access to the data, who are the data recipients (beyond the enterprise), how long the data will be retained, and who will be informed in what cases [19], [24].

While conducting business, consumers evaluate the organizations' privacy protection procedures by reading privacy policies [6, chapter 15], [34]. Privacy policies found today on the Internet and otherwise are very abstract [24]. Various studies have shown that the privacy policies on the Internet are long, legalistic and difficult to understand [2], [35]. These reasons tend to make consumers not to read the privacy policies [14]. Privacy policies lack standardization (e.g. vocabulary) and they are not always accessible from a company's main home page [5]. Privacy policies represent the internal data flow in the organizations also; Ann Cavoukian in her book *The Privacy Payoff* highlights the importance of representing and mapping the data flow in

a machine-readable format [8, pp.286]. Hence, these human-readable privacy policies need to be converted into machine-readable policies and preferences so that software agents can manage the policies for the organizations and consumers, and make decisions for both organizations and individuals.

1.4 Platform for Privacy Preferences (P3P)

P3P was one of the first languages developed to represent the human-readable privacy policies into machine-readable policies.

> P3P enables web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents allow users to be informed of web site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate [10], [11].

P3P is currently implemented in Internet Explorer 6 and Netscape 7. Privacy bird is one of the user agents developed to read P3P policies at all P3P enabled sites automatically. Privacy Bird provides an output according to the match and mismatch of the organization's privacy policy and privacy preferences of the user. According to the match and mismatch of policies the bird provides the following symbols [13]:

- A happy green bird indicates a site that matches a user's preferences,
- The same green bird with an extra red exclamation point indicates a site that matches a user's preferences but contains embedded content that does not match or does not have a P3P policy,
- A confused yellow bird indicates a site that does not have a P3P policy,
- An angry red bird indicates a site that does not match a user's preferences, and
- A sleeping gray bird indicates that the tool is turned off.

Few other resources on P3P are: [3], [4], [21], [22], [35].

Privacy Finder is a privacy-enhanced search engine; the search results are based on the comparison of the computer-readable privacy policies of

organizations against the users' privacy preferences. Privacy finder makes use of some privacy bird symbols mentioned above while showing the results [30].

1.5 Privacy risks from personalization

Personalization helps organizations to build and retain relationships with customers, but it also raises a number of privacy concerns. One of the main concerns among the public regarding personalization is the unsolicited marketing. Telephone calls, emails and physical mails have been of high concern to public. Personalization provides both advantages and disadvantages for the users. The level of personalization in the following areas can pose high level of concerns among the public:

- Wireless location tracking,
- Semantic web applications, and
- Ubiquitous computing.

The kind of personal information that the organizations like Amazon and Google knows about the users is alarming. Different technological solutions have been provided to protect the personal information of the individuals. These technologies are called Privacy Enhancing Technologies (PETs). PETs help in increasing the privacy protection of consumers by providing adequate information to consumers thereby helping them to make informed decisions [8]. P3P discussed earlier is one of the Privacy Enhancing Technology.

In particular, personalization of websites is necessary for users to obtain some customized services from websites, but there is a threat of loosing privacy in gaining customized service. Websites follow various techniques to provide personalized service to the users, some of them are privacy-friendly but most of them could be directly or indirectly privacy-invasive.

The privacy risks raised by personalization cannot be reduced by single approach and there needs to be multiple approaches to reduce the risks of personalization. Two of the approaches are:

- **Reduce data collection and storage**: In this approach, according to the collection limitation principle described earlier, only necessary data is collected and stored. Organizations should always try to reduce the information that is being collected from the users.

- **Put users in control**: In this approach, the user is given reasonable default rules with the ability to add / change rules for handling specific data (up front / with each action / after-the-fact). Also the user is provided with explicit privacy preference prompts during transaction. Users should be given the option of making use of different personas. The approach of providing different persona will help users to keep different identity in different situations (e.g. work and home).

Both technology and policy together can provide a better solution for the privacy invasiveness problem during personalization [12], [25].

2 Take away points

- Privacy is a fundamental need for human beings; privacy has different definitions; the definition of privacy is context specific.
- In legal terms, there are different approaches using which the personal information of the users can be protected (privacy laws and self-regulation). Understanding of privacy in different parts of the world is different. There is no uniform international law to protect privacy in all countries.
- Privacy policy is a means by which the consumers get to know about the privacy practices of the organizations.
- Different technologies have been developed to protect privacy of the consumers and to help users make informed decisions. Platform for Privacy Preferences (P3P) is one such technology.
- Personalization helps organizations to build and retain relationships with customers, but it also raises a number of privacy concerns. Different approaches can be used to protect the customers privacy while providing personalized service.

References

[1] Aftab, P. *The Parent's Guide to Protecting Your Children in Cyberspace.* McGraw-Hill Companies, 1999.

[2] Anton, A. I., Earp, E. A. J. B., Bolchini, D., He, Q., Jensen, C., and Stufflebeam, W. The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. *IEEE Security and Privacy 2(2)* (2004), pp. 36–45. Retrieved Dec 20, 2004, http://www.theprivacyplace.org/papers/glb_secPriv_tr.pdf.

[3] Ashley, P., Hada, S., Karjoth, G., and Schunter, M. E-P3P Privacy Policies and Privacy Authorization. In *WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society* (New York, NY, USA, 2002), ACM Press, pp. 103–109.

[4] Beres, Y., Bramhall, P., Mont, M. C., Gittler, M., and Pearson, S. On the Importance of Accountability and Enforceability of Enterprise Privacy Languages. Tech. rep., Trusted Systems Laboratory (TSL), Hewlett-Packard Labs, Bristol, UK, Retrieved June 17, 2005, http://www.w3.org/2003/p3p-ws/pp/hp1.pdf, 2003.

[5] Bolchini, D., He, Q., Antn, A. I., and Stufflebeam, W. I need it now: Improving Website Usability By Contextualizing Privacy Policies. Retrieved Oct 4, 2005, http://www4.ncsu.edu/ qhe2/publications/ICWE2004.pdf.

[6] Cady, G. H., McGregor, P., Cady, G. H., and McGregor, P. *Protect Your Digital Privacy! Survival Skills for the Information Age.* Pearson Education; 1st edition., December, 2001.

[7] Camp, L. J. *Trust and Risk in Internet Commerce.* The MIT Press, April 18, 2000.

[8] Cavoukian, A., and Hamilton, T. *The Privacy Payoff, How Successful Business Build Consumer Trust.* McGraw-Hill Ryerson Trade., 2002.

[9] COPPA. Children's Online Privacy Protection Act of 1998. Retrieved June 24, 2005, http://www.ftc.gov/ogc/coppa1.htm.

[10] Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., and Reagle, J. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. Retrieved Nov 10, 2004., http://www.w3.org/TR/P3P/.

[11] Cranor, L. F. *Web Privacy with P3P.* O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2002.

[12] Cranor, L. F. I Didn't Buy it for Myself: Privacy and Ecommerce Personalization. Retrieved Nov 25, 2004, http://lorrie.cranor.org/pubs/wpes03.html.

[13] Cranor, L. F., Guduru, P., and Arjula, M. User Interfaces for Privacy Agents. Retrieved Jan 25, 2006, http://lorrie.cranor.org/pubs/privacy-bird-20050714.pdf.

[14] Culnan, M. J., and Milne, G. R. The Culnan-Milne Survey on Consumers & Online Pri-vacy Notices. Retrieved Sep 13, 2005, http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf.

[15] Department of Justice, Canada. Privacy Act. Retrieved June 24, 2005, http://laws.justice.gc.ca/en/P-21/95414.html.

[16] EconomicTimes. IT Act Review Panel to submit report. Retrieved June 28, 2005, http://economictimes.indiatimes.com/articleshow/1152691.cms.

[17] Etzioni, A. *The Limits of Privacy.* Basic Books., April 2000.

[18] European Union Council. The European Privacy Directive. Retrieved June 24, 2005, http://austlii.edu.au/ graham/PLPR_EU_1.html.

[19] Federal Trade Commission. Privacy Online: A Report to Congress. Retrieved July 25, 2005, http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[20] Fogg, B. *Persuasive Technology: Using Computers to Change What We Think and Do.* Morgan Kaufmann., December, 2002.

[21] Grimm, R., and Rossnagel, A. Can P3P Help to Protect Privacy Worldwide? In *MULTIMEDIA '00: Proceedings of the 2000 ACM*

workshops on Multimedia (New York, NY, USA, 2000), ACM Press, pp. 157–160.

[22] Hochheiser, H. The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context. *ACM Trans. Inter. Tech. 2*, 4 (2002), 276–306.

[23] Hofstede, G. *Cultural and Organizations - Software of the Mind - Intercultural Cooperation and its importance for survival.* McGraw-Hill., 1991.

[24] Karjoth, G., and Schunter, M. A Privacy Policy Model for Enterprises. In *the proceedings of 15th IEEE Computer Security Foundations Workshop, 2002.* (2002), pp. 271 – 281.

[25] Kobsa, A., and Cranor, L. Conference proceedings of Privacy-Enhanced Personalization (PEP2005). Retrieved Nov 25, 2004, http://www.isr.uci.edu/pep05/papers/w9-proceedings.pdf.

[26] Kumaraguru, P., and Cranor, L. F. Privacy Indexes: A Survey of Westin's Studies. Tech. rep., Carnegie Mellon University, Retrieved Dec 25, 2005, from http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf, 2005.

[27] Kuner., C. *European Data Privacy Law and Online Business.* Oxford University Press., 2003.

[28] Office of Legislative Drafting and Attorney-Generals Department, Canberra. Privacy Act 1988. Retrieved June 24, 2005, http://privacy.gov.au/publications/privacy88_030504.pdf.

[29] Organisation for Economic Co-operation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved July 27, 2005, http://www.oecd.org/document/18/0,2340 en_2649_34255_1815186 _1_1_1_1,00.html.

[30] Privacy Finder. Privacy Finder. Retrieved Jan 25, 2006. http://search.privacybird.com/.

[31] Privacy of Consumer Financial Information. The Gramm-Leach-Bliley Act. Retrieved June 24, 2005, http://ftc.gov/privacy/glbact/glboutline.htm.

[32] Robert Ellis Smith. *Ben Franklin's web site : privacy and curiosity from Plymouth Rock to the internet.* Privacy Journal, 2000.

[33] Schwartz, P. M., and Reidenberg, J. R. *Data Privacy Law: A Study of United States Data Protection.* Michie, 1996.

[34] Smith., D. *A Survival Guide in the Information Age : 145 Important Tips to Protect You and Your Family.* Longstreet Press., April 25, 2004.

[35] Stufflebeam, W. H., Ant, A. I., He, Q., and Jain, N. Specifying Privacy Policies with P3P and EPAL: Lessons Learned. In *WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society* (New York, NY, USA, 2004), ACM Press, pp. 35–35.

[36] United States Department of Health & Human Services. United States Department of Health & Human Services. Retrieved July 13, 2005, http://aspe.os.dhhs.gov/_/index.cfm.

[37] Warren, S., and Brandeis, L. D. The Right to Privacy. In *Harward Law Review* (Retrieved June 26, 2005, https://netfiles.uiuc.edu/ehowes/www/w-b.htm, 1890).

[38] Westin, A. A Guide to Understanding Privacy. Retrieved Jan 24, 2006. http://www.privacyexchange.org/japan/privacyguide04.pdf.

[39] Westin, A. *Privacy and Freedom.* Bodley Head., 1970.

[40] Westin, A., and Harris Louis & Associates. Harris-Equifax Consumer Privacy Survey. Tech. rep., 1991. Conducted for Equifax Inc. 1,255 adults of the national public.

[41] Westin, A., and Harris Louis & Associates. Health Information Privacy Survey. Conducted for Equifax Inc. 1,000 adults of the national public.