Your Place or Mine?: Privacy Concerns and Solutions for Server and Client-Side Storage of Personal Information

Deirdre Mulligan and Ari Schwartz
Center for Democracy and Technology

The best way for a well-meaning company to avoid a privacy gaffe is to refrain from collecting any personal information.[1] However, while companies should limit collection of information to only what is necessary to complete a transaction,[2] interactions often require more information. Complete anonymity or even pseudonymity are not always desirable. Indeed, software companies and Web site operators have begun to build systems that store personal information. For consumers, these digital "wallets" offer the ability to avoid retyping information such as credit card numbers and shipping addresses. For the businesses, the wallet may be a pure storage device or they may have hopes of customizing, targeting, personalizing and profiling individuals based on this information. While technology alone cannot prevent "bad actor" companies from misusing personal information, systems can be designed to help well-meaning companies build in privacy protections for users.

The products of some companies invite individuals to store personal and perhaps click-stream data on their own server. Other products are designed as wallets or safes to sit on the consumer's own computer. These client-side solutions usually offer the greater potential for user control over information and stronger protections, but both server and client implementations could be built to empower a user or to invade privacy. In each case, decisions to protect privacy need to be embedded in the technology's design.

Server-Side (Su Casa)

Storing personal information on the server-side raises important privacy concerns that client-side solutions do not. These centralized data source offers an easy way to gather large amounts of information from a single source. For example:

- **Government agencies** are given an easy way to sponge off personal information from the private sector. The U.S. government can, in most cases with limited procedural hurdles, access personal information held by private companies. A large database with a lot of personal information provides an unparalleled resource. While the Fourth Amendment provides protections for illegal searches and seizures, these rights have slowly been eroded as information is stored further from the individuals pocket and home in the digital age. A quick glance

at the "Current Legal Standards for Access to Papers, Records, and Communications" chart[3] provided in the appendix of this paper indicates that as personal information moves into a networked environment, individuals lose the Fourth Amendment protections afforded under the constitution.[4]

- **Unscrupulous hackers** also find large databases of personal information inviting. The centralization of information provides them with an easy target. Why would a wrong doer try to pick-off information in transit or hack into individual computers when there is a collection of thousands of similar records in a single place? News stories tell new sordid tales of hackers breaking into e-commerce sites. For example, a hacker recently swiped 300,000 credit card numbers from the CD Universe database and then posted them online when the company refused to pay blackmail money.[5] This simply would not have happened if the information was not stored in a central database.

Even the best-intentioned company storing personal information server-side — keeping only the data necessary to complete transactions — is open to becoming an unwilling source of information for others pursuing different interests. Putting aside the complex security concerns for such a database, even the simple, real-world considerations for handling the database present obstacles. The growth in subpoenas served to online companies seeking information about consumers in both civil and criminal cases serves to prove this point.[6]

Some companies, intent on preserving server-side implementations, have begun to build solutions that take the liability of holding this information away from the company by offering controls only to the user. Several such systems have been designed using different techniques.

These implementations offer similar variations on the same theme. The companies encrypt the database, creating a safe where only the individual with the proper authentication can enter.[7] The company would not have access to any of the information and therefore the ability of outsiders to demand access is limited. These companies can not turn the information over to government authorities, because they are not able to. Large hacks of the whole system would be difficult if strong encryption is used.

Client-Side (Mi Casa)

Client-side systems offer the simple benefit of distributed information. By not aggregating in a central location, the systems limit their attractiveness to lawyers, litigators, government and hackers. While client-side storage seems the more obvious route to protect privacy, using such a system does not by any means assure security or privacy. However, when all of the personal information is stored client-side, the user could be anonymized to the service provider; some personal information could be encoded (e.g., preference information could be given a number code, blue=1, green=2); and, of course, all encrypted. This would minimize the damage from any in transit reception or accidental misuse.

Client-side solutions also instill a greater sense of user trust. Privacy has been identified as the main concern keeping new users off of the Net.[8] A company building software solutions would want to be able to assure users that they have as much control over their information as possible. It is easy for a consumer to understand that their personal information will stay under their control at all times.

The main problem for client-side systems is that they are not portable. If all your personal information is stored on a home computer, it doesn't help you in surfing during your lunch break at work (Imagine if your real wallet were chained to your desk). Smart Cards or other portable devices could solve this problem. The information could be stored on a portable system, as it would be on a hard drive of a desktop computer. The downside would be in insuring the basic technology used to

support the device prevents the sharing of information and insuring a diversity set of devices, so as to avoid their devolution into a de facto national or international ID or system.

Footnotes

[1] We are using a broad definition of personal, meaning identifiable: the use of information relating to an individual that identifies that individual — this may include linking information with personally identifiable information from other sources or combining information so as to infer a person's identity. That is: name, address, ID number, etc. as well as IP address, email address, psychographic information, etc.

[2] In fact, Germany requires collection limitation as part of its data protection law. The Organization of Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data principles < http://www.cdt.org/privacy/guide/basic/oecdguidelines.html>, adopted by hundreds of countries and companies, includes "collection limitation" as its first principle. Roger Clarke of Xamax consulting Pty. Ltd. in Australia has done some excellent work in helping build guidelines to determine when the collection of personally identifiable information is needed for authentication purposes. Clarke's work on this subject is available at http://www.anu.edu.au/people/Roger.Clarke/EC/.

[3] CDT Senior Staff Counsel, James X. Dempsey, created this chart. Representatives of the Department of Justice agreed upon the accuracy of the chart, so it actually does represent the current state of the law, not just CDT's view. An online version is available at: http://www.cdt.org/privacy/govaccess/accesschart.shtml.

[4] Senator Leahy (D-VT) has a bill in Congress that could close some, if not many, of these holes (S. 854 or the E-RIGHTS Act of the 106th Congress).

[5] Markoff, John. "An Online Extortion Plot Results in Release of Credit Card Data." New York Times. January 10, 2000. p. A1.

[6] While companies are reluctant to share exact statistics on this subject, we have anecdotal evidence that legal departments have exploded at online companies specifically to deal with this issue.

[7] Password technologies are clearly not the best authentication technique for such a system, but in reality they are currently the most often used. When password technologies are usedin such systemsnow, the companies have the ability to issue new passwords but no ability to see what the passwords are.

[8] Business Week/Louis Harris, "3/16/98 BW/Harris Poll: Online Insecurity," http://www.businessweek.com/1998/11/b3569107.htm

CURRENT LEGAL STANDARDS FOR ACCESS TO PAPERS, RECORDS, AND COMMUNICATIONS

CENTER FOR DEMOCRACY and TECHNOLOGY
1634 I Street, NW Suite 1100 • Washington, DC 20006 • telephone 202.637.9800 • facsimile 202.637.0968 • info@cdt.org • www.cdt.org

What Information Can the Government Get About You, and How Can They Get It? *Version 2.2*

Green = strong privacy protection
Amber = modest or intermediate protection
Red = little or no protection

		For real-time interception, does gov't need a court order issued on (high) probable cause standard ?	For immediate seizure, does gov't need a warrant issued on (high) probable cause standard ?	Can gov't use a subpoena, issued on (low) relevance standard ?	At time of search / subpoena, must gov't give notice to the customer / subscriber to whom the information pertains ?	Origin of rule
TRADITIONAL RECORDS	**PAPERS** Papers in your home or office (record subject = record holder)	N/A	YES, 4th Amendment CAVEAT: Employee rights are limited	YES CAVEAT: Employee rights are limited	YES CAVEAT: Some courts allow "sneak & peek"	Bill of Rights, 1791
	DATA Electronic data stored on your hard drive or disks at home or office (record subject = record holder)	N/A	YES, 4th Amendment CAVEAT: Employee rights are limited	YES CAVEAT: Employee rights are limited	YES CAVEAT: Some courts allow "sneak & peek"	Bill of Rights, 1791
	VOICE Voice in transit (face to face or phone calls)	YES, 18 USC 2510-22 ("Title III")	N/A	N/A	NO, notice is always delayed	Title III, 1968
EMAIL	**EMAIL** Electronic communications (e-mail or other data) in transit (grabbing bits off the wire)	YES, 18 USC 2510-22 ("Title III")	N/A	N/A	NO, notice is always delayed	ECPA, 1986
	EMAIL Unopened electronic communications (e-mail or other data) in storage with provider of electronic communications service to the public incident to transmission for 180 days or less	N/A	YES, 18 USC 2703(a) CAVEAT: Employee rights in e-mail on company system may be limited	NO	NO, 18 USC 2705 (b)	ECPA, 1986
	EMAIL Opened e-mail maintained for 180 days or less by provider of electronic communications service to the public	N/A	YES, 18 USC 2703(a), but may not be necessary	? Some argue YES, that 2703(b) applies	NO, if warrant is used; YES, but can be DELAYED, if subpoena is used	ECPA, 1986
	EMAIL Opened or unopened electronic communications in storage for more than 180 days with provider of service to the public	N/A	NO, warrant can be used, but subpoena suffices 18 USC 2703(b)	YES, 18 USC 2703(b)	NO, if warrant is used; YES, but can be DELAYED, if subpoena is used	ECPA, 1986
THIRD PARTY / NETWORKED	**PHONE LOGS** Transactional records identifying subscribers and telephone toll records	N/A	NO, warrant can be used, but subpoena suffices 18 USC 2703(c)	YES, 18 USC 2703(c); cf. 18 USC 3121 (pen register statute for real-time telephone dialing info)	Notice not required, not even delayed notice	1979, 1986
	EMAIL LOGS More revealing transactional records (e-mail logs,cell phone location info)	N/A	NO, court order issued on relevance std under 2703 (d) is sufficient	NO	NO	CALEA, 1994
	DATA Electronic data in storage on remote server, with person who provides "remote computing service" to the public	N/A	NO, warrant can be used, but subpoena suffices 18 USC 2703(b)	YES, 18 USC 2703(b)	NO, if warrant is used; YES, but can be DELAYED, if subpoena is used	ECPA, 1986
	BANK RECORDS Bank records in hands of bank	N/A	Warrant can be used, but subpoena suffices	YES	Notice can be delayed	1976, US v. Miller, Right to Financial Privacy Act
	SELECTED RECORDS There are special laws for some records — video, cable, educational, etc.	N/A	Warrant can be used, but subpoena suffices	YES	Varies	Various
	CABLE VIEWING		Clear and convincing evidence, reasonable suspicion	NO	YES	47 USC 551
	MAIL / PAPERS Regular mail, email, or papers held by intended recipient — treated as ordinary business records	N/A	NO, warrant can be used,but recipient can voluntarily disclose too	YES, but recipient can voluntarily disclose too	NO	1976, US v. Miller
	CRYPTO KEYS Escrowed keys or other decryption assistance	Court order works, 18 USC 2518(4), but agent can voluntarily disclose too	NO, warrant can be used, but key agent can voluntarily disclose too	YES, but key agent can voluntarily disclose too	NO	1976, US v. Miller
	OTHER RECORDS Store purchases; medical records; hotel and car rental records; networked financial data; etc.	N/A	NO, warrant can be used, but record holder can voluntarily disclose too	YES, but record holder can voluntarily disclose too	NO	1976, US v. Miller
OVER SEAS	Voice, e-mail, or data intercepted in transit or seized from storage medium overseas	N/A, Title III has no extraterritorial effect	N/A, 4th Amendment warrant clause has no extraterritorial effect	N/A	NO	1968, 1990