CERIAS Tech Report 2006-36
The Balance of Privacy and Security
by Eugene H. Spafford and Annie I. Anton
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

The Balance of Privacy and Security[1]

Eugene H. Spafford
Purdue University CERIAS
spaf@purdue.edu

Annie I. Antón
NC State Univ / The Privacy Place
aianton@ncsu.edu

Introduction

In early 2006, reports surfaced in the media of large scale, clandestine, eavesdropping on telephone communications being performed by the U.S. National Security Agency for purposes of counter-terrorism. This followed on earlier controversial efforts such as the DARPA Total Information Awareness Program [And04] and the Transportation Security Administration's Secure Flight Initiative [SF05]. All of these programs collected and analyzed vast amounts of data on large segments of the population with a stated purpose of trying to identify terrorists. This has resulted in public outcry because many view this as an invasion of privacy and one that might not accomplish its purported goal [Sti05]. Moreover, the availability of this data raised concerns about the potential for other unauthorized or unwarranted uses thereof. This chapter examines the tension between Internet privacy and legitimate needs of law enforcement.

Much of what we do in today's society involves information exchange and surveillance; for example, government, commerce, healthcare, education and entertainment. However, for people to be comfortable and willing to take full advantage of IT (Information Technology) services we need to safeguard their privacy and identity. Privacy is important because it helps us maintain our individuality, autonomy and freedom of choice. Individuality is what distinguishes us from others. Autonomy enables us to freely and independently perform every day tasks and activities without feeling that we must act differently because of unwanted external influence or control by others. Some would argue that surveillance in certain contexts can erode one's autonomy and liberty. Security technologies such as surveillance are making it easier to invade people's privacy. In the past, these technologies were discussed within the context of spying on the enemy or deterring crime. However, the ubiquity of security technologies today has brought the ability to engage in spy-like activities to the masses. Technology has made it easy, simple and cheap to collect, store and search data. Consequently, we observe an escalating tension between those who are eager to use security technologies and those who value privacy as an inherent right and distrust those who monitor their activities. Whatever the context, once privacy is lost it can seldom be fully recovered.

A Basic Conflict

The Internet is a powerful mechanism for distributing ideas, images, sound, and other intellectual content with low cost and great rapidity. It provides a means for collaborative development of artifacts, either in real time or incrementally, and enables "time shifting" so that the audience can choose the time and place to peruse posted content. These characteristics provide a means for a "marketplace of ideas" (as articulated by Holmes and Brandeis in 1919 in

---

[1] A version of this was published as chapter 8, pp. 152–168 in *Controversies in Science and Technology, Volume II*; ed. D. L. Kleinman, K. A. Cloud-Hansen, C. Matta, and J. Handelsman; Mary Ann Liebert, Inc., New York, NY; 2008. Also published as CERIAS Technical Report TR 2006-36.

the dissenting opinion in the case Abrams v. US) that makes it possible for anyone who can afford time at an Internet cafe to publish without having to be a traditional publisher.

Within a large enough population there will likely be those with interests that do not meet the definition of "lawful" or even "sane" as articulated by the majority. Thus, the potential emergence of communication streams devoted to criminal enterprises, prurient (or deviant) interests, radical or revolutionary political expression, bigotry and hate speech, and more. It may well be that some of the individuals pursuing these streams are mentally disturbed and sociopathic in nature. Unfortunately, the same Internet that allows them to exchange ideological texts also allows them to formulate joint plans, obtain technical information, and order dangerous materials. Given the fragility of many of our social and technical systems, and the widespread availability of technologies that may be used offensively, it is in the interest of law enforcement and government, as representatives of the people, to discover and prevent offenses before they occur.

As individuals, we decide what is offensive, but as a society we define offenses. At what point does something actually become "an offense"? Individuals who are unhappy with the government should be free to express displeasure with their officials and disdain with their actions. Invective may even help diffuse anger over official actions (and misdeeds), and act as a cathartic. The United States has the notion of free speech as a cherished right of the public, and the government is prohibited from exercising prior restraint. Even the act of officially observing such speech, or forcing the identification of the speaker (or author) may restrain such speech, and has been prohibited by courts in some venues.

There are other reasons why an author or speaker may wish anonymity beyond simply voicing political discontent. Discussing information about matters that may be viewed as highly secretive, such as issues about medical conditions, religion or sexuality, can be hampered by observers matching the questions with the questioners or responders. Individuals raising issues of public safety ("whistle blowers") may fear for their financial or personal safety and seek to report anonymously in a public forum. Those who have suffered physical, mental or sexual abuse may wish to share their stories as both therapy and guidance for others without the chance of damaging their images as held by those who know them.

In these, and other cases, private conversations preserve something of value to the participants. Truly anonymous posting helps to encourage openness and honesty by participants without fear of retribution. However, we cannot tell, a priori, if those conversations are socially-benign or of a more egregious nature. Thus, we cannot determine in advance whether a conversation should have the strongest possible privacy protections, or some more penetrable form of protection. When made as a default choice of privacy (non)protection, the choice colors all subsequent communications, for good or ill.

In addition to the choices made for the privacy of personal communication, we also see choices made for the privacy protection of messages by organizations and governments. Those organizations are also capable of misdeeds that can be concealed by undue secrecy. Because of their additional resources, misdeeds by government and organizations may be broader in scope and more difficult to redress. Exposure of operations and behavior of these entities provides a check on their potential misbehavior. However, complete transparency is not desirable because those organizations maintain information on individuals that must be kept private, and they handle sensitive information that is necessary both for competitive advantage and security. The

use of computing for data storage and processing, for communication, and for process control greatly complicates the ability of these organizations to protect their information from prying eyes, but also provides new opportunities for visibility into their operations.

Security and privacy are not opposites, but their interests often conflict. The increasing use of information technology may amplify those conflicts. In the following sections we will outline some of the conflicts that have arisen in recent years regarding the use of Internet communications.

What Is Privacy?

There is no absolute definition of privacy as it means different things to different people. Within the context of information collection, storage and use, we define privacy as the expectation that information about you, as an individual or as member of a group, and which is not generally known, will not be disclosed. This can include your activities, your name, your affiliations and other information about you. In today's world of ubiquitous technology, this information spans anything from your telephone records to your medical history. It is important to emphasize that the definition of privacy depends on what you do not want revealed about you to others, and that this is subjective. Some people are "open books" whereas others are very private individuals. In American society, the tradition has been to support whatever view of privacy different individuals may have. Exceptions to this come into play for purposes of public health, public safety and law enforcement. However, despite the apparently clear language of law, this is interpreted subjectively. An example in 2006 was the controversy of the U.S. government wiretapping the phones of suspected terrorists [Cau06]. Individual beliefs concerning whether government should be able to compel us to provide information about ourselves differs from person to person.

There are valid social reasons why ones privacy may be intruded upon, such as when a child is suspected of being a victim of abuse, or to investigate or prevent criminal activity. Generally speaking, people's perceptions of privacy and privacy invasions are relative to materials and timing. For example, some people view any unsolicited email as an intrusion whereas others are happy to have 24-hour web cams in every room of their houses. For purposes of this discussion, we thus consider any information that you do not want revealed about yourself to be a privacy invasion because, for example, if revealed it may cause you to change your behavior. If an information disclosure is not damaging to you, but it still causes you to change your behavior, it is an intrusion; for example, purchasing items in cash so that they cannot be tied to you (e.g. magazines, alcohol, etc.) or to ensure that others will not treat you differently is a means of protecting your privacy.

Identification

A time-honored method of protecting individual privacy is the use of anonymity. Throughout recorded history materials have been written under pseudonyms to protect the author, such as was done with the Federalist Papers [HJM87] in the early American colonies. To this day, the authorship of some of those papers --- viewed as foundations of U.S. political thought -- is still uncertain. Anonymity in political expression is still a major concern of self-preservation: Political dissidents in many countries around the world today are subject to arrest, torture, and possibly execution if their identities are discovered.

Pseudonyms offer another way to protect ones privacy; pseudonyms may promote the consideration of the ideas expressed independent of any existing reputation or image of the author. For example, Mary Anne Evans used the pseudonym George Eliot to hide that she was female because she wanted her work to be taken seriously and because she wanted to guard her private life from the public. Similarly, Charles Dodgson used the pseudonym Lewis Carroll to hide that his fiction was written by a mathematician. In online games and discussion groups individuals often choose personas that portray different ages, genders, or ethnicities so as to relate in ways independent of their actual selves. Adolescents, in particular, may use these pseudonymous identities as a way of helping them to refine their own real identities and interests.

Although anonymity is often used to conceal one's identity for legitimate reasons, anonymity can also be misused. Libelous and hurtful statements may be made anonymously that cannot be easily refuted, nor can the authors be held accountable for the harm caused by their falsehoods. Impersonation of others to commit fraud is a significant form of criminal activity. Stalking and solicitation of minors by sexual predators are two crimes that occur all too frequently online, and which are often difficult to investigate and resolve when pseudonyms or anonymous communication is involved. Communication within loose organizations of criminals trading in stolen intellectual property or access codes is difficult or impossible to investigate without knowing the underlying identities of participants.

For anonymous participation to succeed in those cases where it is most needed, such as under threat of financial or political retribution, the anonymity needs to be so strongly protected as to be effectively inviolable. However, because we cannot know a priori whether such communication is lawful or harmful, there is a basic conflict — do we support mechanisms that allow for true anonymity to anyone seeking it, or do we force all participants to have some form of (eventually) verifiable identity?

Log Analysis and Data Mining

The pattern of someone's behavior can reveal a great deal about what they are doing. For example, given the information that someone has used a search engine to search on a term such as "Fanconi's syndrome," followed by visits to WWW sites on bone marrow registries and information on "antithymocyte globulin" may well lead to a likely conclusion that the person's child has been diagnosed with aplastic anemia. This inference, even if incorrect, could be viewed as an invasion of privacy by the person doing the searches. Other inferences can be drawn based on items purchased online, patterns of email received, and even the times at which the accesses occur. The results of such inferences could be used for directed marketing, public health studies, or to reduce the coverage available under a health insurance policy. They might also be used for targeted fraud ("phishing") or extortion.

If the subject making the searches is a researcher working for a large pharmaceutical firm, observation of the searches performed might provide clues about current research interests and drug development. When employed by a competitor this form of surveillance can be used to "scoop" development on a new product. The financial incentives for such inferences can be quite significant in a number of industries, and may drive some agents to also employ illegal means of observation.

Law enforcement has proposed use of similar techniques to identify criminals. By observing who has a history of seeking information on hydroponics and purchasing high-intensity daylight spectrum lights, drug enforcement agents hope to find people with clandestine marijuana growing operations. By observing who has a history of research into explosives, purchases of nitrogen fertilizer, and on-line searches of building plans, some Federal agents hope to identify terrorists before they strike. In both cases there is a presumption of guilt based on purely circumstantial evidence, and the searches and inferences are likely to be viewed as an invasion of privacy by anyone incorrectly targeted for law enforcement activity.

Some policy makers want to require ISPs and online services to keep extensive logs and records of user behavior so that criminals such as child pornographers and identity thieves might be traced and prosecuted. However, keeping such extensive records would potentially allow others to gain access, for reasons of civil litigation, directed marketing, or criminal activity. The potential for accidental disclosure of these stored records is also a concern. For instance, the Privacy Rights Clearinghouse announced in December 2006 that over 100 million personal data records had been disclosed or compromised in a two year period – records that were presumably better protected than ISP logs because of their more sensitive nature.[2]

Long Term Storage & Processing

Historically, information that was stored for long periods of time was generally information that had been analyzed and synthesized, or had proven value. Data without known value was often not collected nor saved because of the cost of storage media and space. Also, the process of manually indexing large data stores so as to find specific items at some future time was itself time-consuming and difficult. As such, the whole process of collecting and storing data had some built-in limits.

Currently, modern computer storage of information is relatively inexpensive, and indexing and advanced searching are performed by advanced algorithms and fast computers. There are currently few disincentives to storing significant quantities of data, including personal data. At the same time, advances in data mining and matching technologies provide for massive data searching and inference formation. It is possible to derive previously unknown correlations and patterns from massive collections of data. Depending on the agency performing the searches, these correlations may provide new insights into a range of issues such as disease transmission and epidemiology, tendencies to vote for particular political candidates, the likelihood of buying certain sets of products, or social networks of criminals.

Clearly, there are strong reasons that such data would be collected, saved and sold to new aggregators. Governments would want the data so as to anticipate citizen needs and provide needed services, law enforcement would want the data to identify malfeasors, and commercial entities would want to use the information for purposes of advanced marketing and pricing. Historians and other social scientists would also find detailed data to be of value in understanding events and trends. However, the collection and use of such information facilitates intrusions into privacy of individuals and groups. Not only is it possible to discover information in the data (and its relationships) about individuals, but erroneous information also presents possibilities for intrusions. Transcription errors, old (stale) data, and simple errors in algorithms

---

[2] <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

used to process the data may result in both type I (false positive) and type II (false negative) errors. Actions taken on erroneous conclusions may result in everything from mis-targeted advertisements to false accusations of criminal behavior — all of which would be considered to be (at least) privacy violations. These are often all the more surprising to the subjects when they discover the extent to which data about them has been saved.

Unfortunately, the propensity for errors and inaccuracies in the information that data brokers collect is exacerbating the problem. Studies have revealed that data broker files are riddled with errors and that there is no easy way to fix these errors [Sul05]. Moreover, a recent study examined the quality of data provided by ChoicePoint and Acxiom [PA05]. Of the reports given out by ChoicePoint, 100% had at least one error in them. The error rates for basic biographic data (including information people had to submit to receive their reports) fared almost as badly: Acxiom had an error rate of 67% and ChoicePoint had an error rate of 73%. The majority of participants in the study had at least on significant error in their reported biographical data from each data broker.

Resolution?

It is clear that there are a number of privacy-related conflicts relating to the collection, storage, analysis, and use of information in computing systems and networks. Most of these conflicts are rooted in fundamental differences of opinion about the role of privacy and the grounds under which the veil of privacy may be lifted. Because there is such a range of circumstances under which these determinations may be made, and because many cannot be determined in advance (as illustrated in the examples, above), we are left with an environment where deployment of technology and establishment of policy must be guided by principles that are designed to protect privacy yet allow for legitimate uses of personal information by others.

In early 2006, in response to a steady stream of privacy breaches and news accounts of significant government programs to surveille and analyze citizen information, the US Public Policy Committee of the ACM created a set of privacy recommendations. The ACM is the oldest scientific and professional organization for computing professionals, with almost 80,000 members worldwide. The privacy recommendations were created based on professional experience, previous recommendations such as the Fair Information Practices [Wa73], and current law in many countries around the world (e.g., the Canadian Privacy Act[3]). The committee sought to codify best practices that would maximize transparency and accountability, reduce error and surprise, minimize the potential for misuse and data exposure, and yet also allow reasonable continued and future use of aggregated data by business and government. The 24 recommendations are shown in Box 1, grouped by major concept.

The ACM Privacy Recommendations represent an attempt to balance enhanced personal privacy with legitimate use. The following are examples, one from each major grouping:

> Minimization, #2: *Store information for only as long as it is needed for the stated purposes*. This principle recognizes the need for organizations to store personal information for various uses. However, to reduce the time during which that information may be exposed, and to reduce the potential amount of information that may be exposed, the principle states that information should only be kept until its defined uses are met.

[3] <http://www.privcom.gc.ca/legislation/02_07_01_01_e.asp>

Too often, organizations collect information and then keep it indefinitely because "it might be useful later." This leads to information drift (becoming less accurate) and increases the potential for disclosure.

This principle implies an assumption that the organization has thought through and formulated an explicit privacy policy, and a definite set of use cases for the collected data – two exercises that are conducted by too few organizations

Consent, #7: *Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information*. When individuals provide information (or they are informed that it is collected), it should be with a set of stated purposes and policies about how it is used. The individual can choose to consent or not under those circumstances, or to file objections with the organization through appropriate channels. If an organization later decides to alter those parameters, the individual should be fully informed and given the same chance to consent to participate as when the information was originally collected. This allows organizations to find new uses for already-collected information, without going to the effort of recollecting and validating that information. However, it does not allow unrestricted use of the data. Note that the concept of "informed consent" is commonly used in scientific experiments and medicine to ethically determine participation.

Openness, #13. *Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so*. To support informed consent, as per #7, individuals must actually be informed about the uses of their personal information. Other principles in this group stress that the provided information be explicit, bounded, and understandable. However, this principle also recognizes that some law enforcement and government databases may contain information that individuals should not know about – either how it is used, or that they are profiled in those databases. Thus, for good reasons law may exempt disclosure of those databases, but the requirement that those exemptions be defined in law presumes that some appropriate deliberation and oversight has occurred related to making that determination.

Access, #14. *Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so*. One aspect of information collection that frightens or annoys many people is the prospect of inaccurate information being used to make decisions about them. This principle recognizes that concern, and encourages the data holder to provide meaningful mechanisms to allow that information to be examined, and if appropriate, corrected by the individuals involved. We note that this might actually be to the benefit of the organization holding the data because it might lead to a more accurate, and therefore higher quality and more cost-effective, data collection.

This principle is currently supported by too few organizations. For example, ChoicePoint used to state that it could not correct errors in its records, but that consumers must locate the original source from which ChoicePoint gathered the information and correct any mistakes there [OA07]. In contrast, the right to access and correct erroneous financial information has been a part of the Fair Credit Reporting Act since its passage in 1970. Recently, ChoicePoint has announced plans to allow individuals to review and

correct their personal information via a single point of access [Hus05]; however, this system is not yet available to consumers.

As with principle #13, principle #14 recognizes that there may be databases that should not be made known to the subjects, or the extent of the information on them should not be made known during the lifetime of the information. As before, the requirement that the exemption be defined in law presumes that some appropriate deliberation and oversight has occurred related to making that determination.

Accuracy, #18. *Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data*. This matches, in part, with principle #14, and also with #17. It recognizes that data is collected for particular purposes and may be supplied to business partners. Furthermore, it recognizes that data is sometimes shared between organizations for valid purposes, and as allowed by law or policy. As examples, banks provide transaction information to the Internal Revenue Service, and airlines share some flight information with their associated frequent flier programs. When data is shared, this principle requires the holders of the data to propagate any valid corrections rather than make that task a burden on the individuals involved. Further, it is defined as a "push" operation rather than a "pull" operation so that it is more likely to occur when the correction is made, rather than in response to a periodic bulk request.

Additionally, this principle implies that a data aggregator must keep a record where data is shared, and from where it is received. Thus, if an individual discovers and corrects an error in the middle of a "chain" of data sharing, it will propagate to both the initial end sites – the individual does not need to discover each location, or the first location, where the data was collected as currently required by ChoicePoint. This is especially important if some of the data collections are exempt from disclosure or review by the individual; so long as the corrections will traverse the same path as the data that was provided, presumably all copies of the data will be corrected in a timely fashion.

Security, #20. *Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies*. This principle addresses one of the most common and often overlooked routes of exposure of personal information – physical compromise of the data. Too often, IT professionals focus on access control and encrypted communication, but fail to realize that the data they are trying to protect exists in multiple forms in multiple locations, many of which are easily stolen. The holder of the data should be responsible for security of the information in the original database and in any additional copies, in whatever format.

Accountability, #22. *Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations*. Excellent policies and training do little unless they are actually applied. It is not always possible to determine if all policies and safeguards are working correctly 100% of the time simply by observing the system or asking the personnel involved. Mistakes may happen, errors in code occur, and personnel may be careless or untruthful for a variety of reasons. It is important for organizations to conduct meaningful, regular examinations to ensure that privacy policies are being followed, and that deficiencies are appropriately

addressed. Furthermore, making these compliance activities and remediations public will likely increase the confidence and comfort of individuals whose information is held by the organization (presuming that the safeguards are appropriate and found to be working correctly).

So long as people view information as private, and so long as others find some value in the collection and analysis of that information, there are likely to be conflicts. Although the full set of recommendations do not obviate all possible privacy conflicts that may result over use of personal information online and in stored data, they are designed to help to reduce the chance of such conflicts when applied as a whole. What remains to be seen is how many organizations or governments embrace these recommendations.

Closing Discussion

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

Benjamin Franklin, Historical Review of Pennsylvania, 1759

The tension between law enforcement and privacy is unlikely to cease to exist. New laws and regulations governing information collection, use, sharing and storage are sure to be introduced in the years to come. At best, we can hope that decisions about privacy policy will be carefully considered by those who are neither afraid of the results nor advocates for either extreme, and that those decisions are made in an open manner, subject to oversight and comment by an informed public. In addition, policies should be subject to reevaluation and reconsideration to ensure that as technology changes, the existing policies still meet the intended goals.

Government is in a unique position of power over individuals, having the capability to deprive them of their freedoms and even lives. Government likewise is in the position of guarantor of citizen rights. The right to privacy should be strongly protected as a social good. Erosions to privacy can occur unintentionally, but by their nature are difficult to repair because once privacy is lost, it is practically impossible to regain it. Moreover, unintended consequences of small disclosures may be amplified when combined with other disclosures and inferences.

Increasingly, those who violate privacy policies, or who are responsible for privacy breaches, are being held accountable for these transgressions. As long as there are differences in motivation, values and experiences among all stakeholders, we are unlikely to have a society in which everyone behaves according to the law. As such, mechanisms, such as tracing networks of offenders, are needed to identify and prosecute those who violate the laws on which society is based. Furthermore, with differences in societies and their foundational principles, it is likely that some may be at risk of aggression and malice from those in other countries and social settings. Societies need to have mechanisms and procedures in place to defend themselves from such threats.

In the United States, we have found that there is strength in diversity, and great creativity in heterogeneity. American society has benefited by encouraging tolerance and allowing people the freedom to push boundaries, sometimes past the point of comfort for some other individuals and

groups. There is both history and philosophy that encourage us to interfere as little as possible with the exercise of individuals' actions when they are not explicitly hurtful of others. This is consistent with Judge William Brandeis' analysis that "Privacy is the right to be let alone."

References

[And04] S.R. Anderson. *Total Information Awareness and Beyond: The Dangers of Using Data Mining Technology to Prevent Terrorism*, Bill of Rights Defense Committee, http://www.bordc.org/threats/data-mining.pdf, 2004.

[Cau06] L. Cauley, NSA has massive database of Americans' phone calls, *USA TODAY*, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm , May 11, 2006.

[HJM87] A. Hamilton, J. Jay and James Madison. *The Federalist Papers*, 1787-1788.

[Hus05] B. Husted, "Exec: ChoicePoint will be more open," *Atlanta Journal-Constitution*, April 1, 2005, L/N.

[OA07] Paul N. Otto, Annie I. Antón and David L. Baumer. "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information," To Appear: *IEEE Security & Privacy,* 2007.

[PA05] Deborah Pierce and Linda Ackerman. Data Aggregators: A Study of Data Quality and Responsiveness, http://www.privacyactivism.org/ docs/DataAggregatorsStudy.html, May 19, 2005.

[SF05] Report of the Secure Flight Working Group: Presented to the Transportation Security Administration. http://www.schneier.com/secure-flight-report.pdf, September 19, 2005.

[Sti05] S.L. Stirland. Privacy, Security Experts Urge Delay of Passenger Screening System, *National Journal's Technology Daily*, September 22, 2005.

[Sul05] Bob Sullivan. ChoicePoint files found riddled with errors, MSNBC News, March 8, 2005.

[Wa73] Ware, Willis et al. 1973. *Records, Computers and the Rights of Citizens,* Department of Health, Education and Welfare, US Government Printing Office.

Box 1. ACM PRIVACY RECOMMENDATIONS

MINIMIZATION

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.
2. Store information for only as long as it is needed for the stated purposes.
3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.
4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.
5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

CONSENT

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (opt-in); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal information, including when appropriate, the deletion of that information (opt-out). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)
7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

OPENNESS

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.
9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).
10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.
11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.
12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.
13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

ACCESS

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.
15. Provide mechanisms to allow individuals to determine with which parties their information has been shared, and for what purposes, unless legally exempted from doing so.
16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

ACCURACY

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.
18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

SECURITY

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.
20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

ACCOUNTABILITY

21. Promote accountability for how personal information is collected, maintained, and shared.
22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.
23. Maintain provenance — information regarding the sources and history of personal data — for at least as long as the data itself is stored.
24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.