



THESSISMUN 2007

THESSALONIKI INTERNATIONAL STUDENT
MODEL UNITED NATIONS

United Nations General Assembly 3rd Committee Topic Area B

The compatibility of Human Rights protection and State interests: balancing national security and privacy in the case of telecommunications.



UNIVERSITY OF MACEDONIA
THESSALONIKI, GREECE

WWW.UOM.GR/MUN - WWW.THESSISMUN.ORG



When we talk about technology, privacy and justice, a theme consistently sounded in these topics is the impact of technological developments on individual privacy and the ability of our laws to meaningfully protect privacy amidst sea-changes in technology.

Rights to privacy are to remain meaningful in the face of rapid technological changes. This is particularly pressing given the expansion of state power to collect, use and disclose personal information.

It is also urgent given the (inevitable) adoption of information technologies to exploit our personal information in the interests of national security. The technology and practice of data mining in the interests of national security serve to illustrate the challenges to privacy, and privacy laws, raised by information technology.

National interest can be defined as a country's goals and ambitions whether political, economic, military, or cultural. A foreign policy geared towards pursuing the national interest is the foundation of the realist school of international relations. The state's survival and security are considered to be of great importance. Wealth and economic growth and power follow, as well as the preservation of the nation's culture. National security refers to the need to maintain the survival of the nation-state through the use of economic, military and political power and the exercise of diplomacy.

Measures taken to ensure national security include:

1. using diplomacy to rally allies and isolate threats,
2. maintaining effective armed forces,
3. implementing civil defense and emergency preparedness measures (including anti-terrorism legislation),
4. ensuring the resilience and redundancy of critical infrastructure,
5. using intelligence services to detect and defeat or avoid threats and espionage, and to protect



classified information,

6. using counterintelligence services or secret police to protect the nation from internal threats.

Although national security measures are imposed to protect society as a whole, such measures will necessarily tend to restrict the rights and freedoms of individuals. The concern is that where the exercise of national security laws and powers is not subject to good governance, the rule of law and strict checks and balances, there is a risk that "national security" may simply serve as a pretext for suppressing unfavorable political and social views. Taken to its logical conclusion, this view contends that measures which may ostensibly serve a national security purpose (such as mass surveillance, and censorship of mass media), could ultimately lead to a **police state**.

Security can be defined as the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from the external environment. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security.

Types of security

- international security
- national security
- physical security
- home security
- information security
- computing security
- application security
- financial security
- human security
- food security



- airport security
- mall security

Security concepts

Certain concepts recur throughout different fields of security.

- risk - a risk is a possible event which could cause a loss
- threat - a threat is a method of triggering a risk event that is dangerous
- countermeasure - a countermeasure is a way to stop a threat from triggering a risk event
- defense in depth - never rely on one single security measure alone
- assurance - assurance is the level of guarantee that a security system will behave as expected

Communications security (COMSEC): Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, traffic-flow security, and physical security of COMSEC equipment.

- cryptosecurity: The component of communications security that results from the provision of technically sound cryptosystems and their proper use. This includes insuring message confidentiality and authenticity.
- emission security (EMSEC): Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems (computers), and telecommunications systems.
- physical security: The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.
- traffic-flow security: Measures that conceal the presence and properties of valid messages



on a network. It includes the protection resulting from features, inherent in some cryptoequipment, that conceal the presence of valid messages on a communications circuit, normally achieved by causing the circuit to appear busy at all times.

- transmission security (TRANSEC): The component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis (e.g. frequency hopping and spread spectrum).

Surveillance is the monitoring of behavior. Systems surveillance is the process of monitoring the behavior of people, objects or processes within systems for conformity to expected or desired norms in trusted systems for security or social control.

The word surveillance is commonly used to describe observation from a distance by means of electronic equipment or other technological means. For example:

- eavesdropping
- telephone tapping
- directional microphones
- covert listening devices or "bugs"
- Minox subminiature cameras
- closed-circuit television
- GPS tracking
- Bait car
- electronic tagging
- CCTV Images
- military reconnaissance
- Reconnaissance aircraft, e.g. Lockheed U-2
- Reconnaissance satellites
- "trusted" computing devices
- Internet and computer surveillance

However, surveillance also includes simple, relatively no- or low-technology methods such as direct



observation, observation with binoculars, postal interception, or similar methods.

The official and unofficial tapping of telephone lines is widespread.

The contracts or licenses by which the state controls telephone companies means that they must provide access for tapping lines to the communications security services and the police. For mobile phones the major threat lies in the collection of communications data. These not only include information about the time and duration of the call, but also from where the call was made and to whom. These data can be determined generally because the geographic communications cell that the call was made in is stored with the details of the call. But it is also possible to get greater resolution of a person's location by combining information from a number of cells surrounding the person's location.

Mobile phones are, in surveillance terms, a major liability. This liability will only increase as the new third-generation (3G) phones are introduced. This is because the base stations will be located closer together

Computer surveillance

At a basic level, computers are a surveillance target because of the large amounts of personal information that they process and store. Anyone who can access a computer can retrieve information. In case someone is able to install software on a computer system, the computer can be transformed into a surveillance device. Computers can be tapped through a variety of methods, ranging from the installation of actual bugs or surveillance software to the remote interception of the radio transmissions generated by the normal operation of computers. Spyware, a term coined by computer security expert Steve Gibson, is often used to describe computer surveillance tools that are installed against a user's will. High-speed Internet connections have made computers more vulnerable than ever before.



Electronic trails

Modern society creates large amounts of transaction data. In the past this data would be documented in paper records and would leave a "paper trail" but today many of these records are electronic, resulting in an "electronic trail" that is easily reconstructed through automated means. Every time you use a bank machine, pay by credit card, use a phone card, make a phone call from home, or otherwise complete a recorded transaction you generate an electronic record. When aggregated and analyzed, this information can identify individual behavior patterns that describe how you live and work. One way to protect autonomy and individual freedom in a paper-based world is through anonymous transactions, for example by using cash. When transactions are electronic, that anonymity may be lost.

Today, large aggregations of transaction information are assembled by marketing, credit reporting, and other data aggregation companies in order to analyze consumer behavior to determine how companies should manage their marketing or sales strategies, or to assess counterparty "trust" for financial transaction. These data sets are also sold to other companies or to government agencies for additional use. The availability of large data sets of transaction information facilitates the use of automated surveillance or analysis techniques such as data mining to perform dataveillance.

Information security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information, however there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Heads of state and military commanders have long understood the importance and necessity of protecting information about their military capabilities, number of troops and troop movements.



Such information falling into the hands of the enemy could be disastrous. Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about a businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to loss on behalf of the enterprises business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases, it is also a legal requirement, and some would say that it is the right thing to do. For the individual, information security has a significant effect on Privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved much in recent years. As a career choice there are many ways of gaining entry into the field. The field offers many areas for specialization including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science to name a few.

Basic principles of Information Security

Six atomic elements of information

For over twenty years information security has held that three key concepts formed the core principles of information security: confidentiality, integrity and availability. These have been known as the CIA Triad. However, in recent years there has been a growing awareness among security professionals that confidentiality, integrity and availability alone were inadequate. The CIA triad is now being replaced with the six atomic elements of information, they are: confidentiality, possession or control, integrity, authenticity, availability, and utility.

Confidentiality

It is virtually impossible to get a drivers license, rent an apartment, obtain medical care, or take out a loan without disclosing a great deal of very personal information about ourselves, such as our name, address, telephone number, date of birth, Social Security Number, marital status, number of



children, mother's maiden name, income, place of employment, medical history, etc. This is all very personal and private information, yet we are often required to provide such information in order to transact business. We generally take it on faith that the person, business, or institution to whom we disclose such personal information have taken measures to insure that our information will be protected from unauthorized disclosure, either accidental or intentional, and that our information will only be shared with other people, businesses or institutions who are authorized to have access to the information and who have a genuine need to know the information.

Information that is considered to be confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to access, use, copy, or disclose the information, and then only when there is a genuine need to access, use, copy or disclose the information. A breach of confidentiality occurs when information that is considered to be confidential in nature has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information. Confidentiality is a requisite for maintaining the privacy of the people whose personal information the organization holds.

Possession or control

In the example of the stolen laptop containing confidential personnel information, the theft could result in a breach of confidentiality if the thief, or someone else, accesses the data. If the confidential information is never accessed then there isn't a breach of confidentiality. However, the theft of the laptop does result in a loss of possession and control of the information - which could eventually lead to a loss of confidentiality. Information security requires that possession and control of the information, and possession and control of the information processing system, be maintained. The presence of a backdoor or rootkit on a processing system is another example of a loss of control.

Integrity

In information security, integrity means that data can not be created, changed, or deleted without authorization. It also means that data stored in one part of a database system is in agreement with other related data stored in another part of the database system (or another system). For



example: a loss of integrity can occur when a database system is not properly shut down before maintenance is performed or the database server suddenly loses electrical power. A loss of integrity occurs when an employee accidentally, or with malicious intent, deletes important data files. A loss of integrity can occur if a computer virus is released onto the computer. A loss of integrity occurs when an on-line shopper is able to change the price of the product they are purchasing.

Authenticity

In information security, authenticity means that the information is both genuine and original; the information is neither a fabrication nor a copy. For example, in SPAM e-mails, the address of the sender is almost always a forged or fabricated address, meaning that it is usually not the genuine one.

Availability

The concept of availability means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed. The opposite of availability is denial of service (DOS).

Utility

Information has a utility if it is both usable and useful. The value of information is dependant upon its utility. If the information is not useful to the intended recipient of the information it has little or no utility and therefore has little or no value to the intended recipient of the information. Likewise, if the information is not in a usable format it has little or no utility and therefore little or no value. Raw meteorological data has very little utility to a tax accountant but may have a great deal of utility to a Meteorologist. An encrypted data file is useless without the encryption keys necessary to decrypt the file.

Access control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the



access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe." they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. Authentication is the act of verifying a claim of identity.

Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under which conditions. The access control mechanisms are then configured to enforce these policies.

TERRORISM, FEAR & NATIONAL SECURITY

Each terrorist attack seems to prompt renewed calls for tougher laws and more surveillance. Many countries, even without relative incidents or evident danger concerning their territory, tend to take measures to protect themselves from a possible attack.

Concern about terrorism is nonetheless a prominent, if not the primary, driver of public policy in the areas of justice and of public safety. Security against criminal violence (terrorist or otherwise) is part of our human rights framework. But we must not react out of fear or pander to fear. State responses to terrorism must realistically address the scale and nature of the threats. This vital point was well expressed in early 2005 by Justice Michael Kirby, of the High Court of Australia.

“The times now are different. The risks have changed. The technology is new. The weapons are in some ways more perilous. Control over them is more disparate. But the need for prudence and care against over-reacting is as strong today.... We must keep in



perspective the powers of those presently ranged against the Western democracies. This is not a reason for complacency over national security or indifference to violence and risks of violence. But it is a reason for keeping our feet firmly planted on the Australian ground. We should never forget that, to the extent that we exaggerate the risks to national security, we fall into the hands of those who threaten our constitutionalism. To the extent that their threats propel us into demolishing the fundamentals of our liberal democracy, we reward the enemies of our form of government with success. To the extent that we over-react, we proffer the terrorists the greatest tribute.”

The first message is one of proportion. We should found our policies and laws on national security upon sound data alone. We should maintain our prudence, as we have in the past.

The point of terrorism, of course, is to create terror. The public has little information with which to realistically assess the risks of terrorist attack at home. Their uncertainty nurtures the fear that is sown by graphic, in-your-living-room, coverage of terrorist atrocities elsewhere. It has been observed that, as a result, elected officials are likely to feel they have few options in dealing with terrorism. They can hardly be seen to be doing nothing, even though citizens are still far more likely to die in traffic accidents or in accidents in the home than in a terrorist attack. The imperative to action, and thus possible over-reaction, exists because, if terrorists strike and officials are judged to have been idle, public outrage at their apparent negligence or callousness will be extreme. By contrast, if officials are seen to have taken steps to prevent attacks and none occur, they will be credited with having successfully fought terrorism, even if the measures they took had nothing to do with the absence of attacks.

There always lies an incentive for more aggressive and widespread measures that may have little to do with actual risk. It is therefore critically important that officials rigorously apply a rule of rational proportionality in addressing terrorist risks. It is vital that fashion policy and legislative responses to terrorism are taken as dispassionately, rationally and proportionately as possible.

Since 9/11, there have been passed or amended laws in ways that blur the lines between the collection, use and disclosure of personal information for national security purposes and its collection, use and disclosure for other purposes, including what could be called ‘ordinary’ law



enforcement uses. These laws, passed in the name of national security, have made it easier for state agencies to collect personal information for national security purposes and then to use it for other purposes. Amendments since 9/11 empower state officials, in the name of national security, to compel businesses and other private sector organizations to turn over customer information for national security purposes and, sometimes, for secondary law enforcement uses.

Against this background of changes to laws, we have to remember that democracies depend on clear and effective rules that both reflect the essential values of a free society and that are suited to the state activities they are intended to govern.

In considering the impact of national security laws on our rights and freedoms, we must remember the risks in blurring the distinctions between national security and ordinary law enforcement laws and activities. Clear distinctions are especially vital in light of the nature, history and likely future of intelligence-gathering activities and uses, which by their very nature are clouded in secrecy and often enjoy greater leeway in the balance with our rights and freedoms. This is especially vital when one remembers the proposition that a defining characteristic of police states is the blurring of distinctions between law enforcement and national security functions, the danger being that the rule of law eventually gives way to arbitrary decision-making by the authorities, which, however well-intended it may be, can have grave consequences for citizens' rights.

We must urgently turn our attention, moreover, to the implications of information technology for individual privacy and other rights are profound. The days of privacy through practical obscurity are gone or close to it and such privacy protection as once was offered by inefficiencies in information storage and distribution will almost certainly vanish in the coming years:

- New technologies that provide easy access to distributed data and efficiency in processing are obviously challenging to a system that is at least partially based on protecting certain rights by insisting on inefficiencies.
- Steps must be taken now to modernize the approach to privacy if it is to remain viable in the face of the enhancement of government power by from developments in information technology.



THE STATE AS AN INFORMATION CONSUMER

Privacy implications of data mining can best be understood against the backdrop of private sector aggregation and mining of personal information and the near certainty that governments will increasingly be consumers of data flowing from the private sector.

Businesses throughout the world have for some years now turned to increasingly sophisticated data analysis techniques to among other things assess credit risk, market goods and services and manage relationships to their customers. Over the past decade in particular loyalty programs have sprouted up everywhere. Some are operated by businesses on their own behalf while other programs are operated by third parties. Through these programs, businesses are collecting very detailed information about consumers' lives, habits, finances, attitudes, purchasing preferences and so on. The scope and detail of the databases is often, enhanced by information gleaned from public records maintained by governments. These commercial data banks are very often for sale, with large corporations offering those willing to pay an increasingly wide array of information products about consumers.

As mentioned earlier, since September 11, there has been a trend in some countries, toward enhanced state powers to compel production of personal information for national security purposes. Governments also appear to have an increasing appetite for personal information acquired from commercial personal information databases.

The assertion that more data means better intelligence is hard to resist, however doubtful it may be as a general proposition. Yet, as commercial databases continue to proliferate, as they become more and more comprehensive and detailed, and as data storage becomes cheaper and cheaper (tending to make databases life-long in scope), it will be very difficult for the state to resist exploiting the rich lodes of data found in the private sector, never mind in the public sector.



DATA MINING

Governments will want personal data in order to use increasingly powerful computer technologies to create knowledge. Computers can be used in a variety of ways to derive knowledge from analysis of data. These techniques are generally referred to as 'data mining' and they are already in widespread commercial use.

The Congressional Research Service has defined data mining this way:

Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees). Consequently, data mining consists of more than collecting and managing data, it also includes analysis and prediction.

Data mining can be performed on data represented in quantitative, textual, or multimedia forms. Data mining applications can use a variety of parameters to examine the data. They include association (patterns where one event is connected to another event, such as purchasing a pen and purchasing paper), sequence or path analysis (patterns where one event leads to another event, such as the birth of a child and purchasing diapers), classification (identification of new patterns, such as coincidences between duct tape purchases and plastic sheeting purchases), clustering (finding and visually documenting groups of previously unknown facts, such as geographic location and brand preferences), and forecasting (discovering patterns from which one can make reasonable predictions regarding future activities, such as the prediction that people who join an athletic club may take exercise classes).

A key characteristic of data mining is that analysis of an individual's personal information can create new, secondary, information about that person. The hidden patterns and subtle relationships that data mining detects may be recorded and thus become personal information of the individual whose life is being scrutinized and analyzed. Information about an individual's credit history, credit card purchases, law enforcement record or interactions, travel habits and so on may be mined to



derive evidence, or even a finding, that she or he is a possible terrorist who should be put on a terrorist watch list or be kept under surveillance. This new personal information becomes part of the swelling river of data whose channels are, in the private and public sectors, ever-changing and difficult to follow, much less control. The easier it becomes to accumulate and analyze personal information on a massive scale, the greater the potential for intentional or unintentional misuse and error. As data banks and data mining grow in sophistication and extent, each person's life will become more and more open to scrutiny, with further details becoming visible with each new advance in data analysis techniques.

On the other hand, data mining can yield benefits, for example, in the form of improved services and greater efficiency. It may be that data mining will offer benefits for national security, although there should be no assumption as to the benefits -careful research is needed in each case to establish whether benefits can be realized.

There are, however, a variety of concerns associated with data mining, which are heightened when data mining is used by the state for national security purposes. Experts have flagged the risks for a number of years of data mining initiatives have also noted the risks and recommended action.

These risks are generally associated with use of data mining for surveillance of individuals, groups or populations. In the case of individuals or small groups, surveillance may be predicated on suspicion derived from other sources or it may be mass surveillance. Government should assess the risks associated with data mining for surveillance purposes before data mining expands, as it is likely to do, and then act to protect privacy.

DATA MINING RISKS

The privacy risks of data mining are varied in nature and significance. While there is broad consensus in the literature about what the risks are, consensus on a hierarchy of risks is not evident. For this reason, the following outline is selective—not all of the risks are mentioned, they are not presented in any particular order, and they overlap in some respects. The goal is to establish that there are risks and then recommend action, since, when these risks are realized, they can entail real and possibly serious harm to individuals.



An overall concern associated with data mining -and other information technologies- is the tendency to attribute reliability or even infallibility to the products of technology. It is therefore important that the following admonition be rigorously respected when creating and operating data mining projects:

Although these techniques are powerful, it is a mistake to view data mining and automated data analysis as complete solutions to security problems. Their strength is as tools to assist analysts and investigators. They can automate some functions that analysts would otherwise have to perform manually, they can help prioritize attention and focus an inquiry, and they can even do some early analysis and sorting of masses of data. But in the complex world of counter-terrorism, they are not likely to be useful as the only source for a conclusion or decision. When these techniques are used as more than an analytical tool, the potential for harm to individuals is far more significant.

POOR DATA QUALITY

The data quality problem can have a variety of causes. Missing data, fragmented data, outdated information and poorly authenticated or unauthenticated data can all contribute to error. Where data are acquired from commercial sources, data quality may suffer because the information was originally collected for purposes that do not require high accuracy.

Take an apparently trivial example from domestic life. Personal information collected through frequent shopper programs might find its way into databases exploited for national security data mining. Affinity programs do not require high assurances of identification upon enrolment and affinity cards may be shared among family, friends or mere acquaintances. Sharing of affinity cards could, for example, lead to false association of certain purchases or habits, and therefore religious beliefs, with the putative registered shopper. Moreover, the shopper's identity is likely not to have been robustly authenticated at the outset. Use of such data for national security purposes, perhaps in conjunction with other flawed data, may paint an inaccurate portrait of an individual or, as the errors multiply across the class, skew more broadly-based analyses.



DATA LEAKAGE (intentional and accidental)

Like water, information flows and it will find a way to escape. Data can and often will be spilled in a variety of ways. These can include loss or theft of poorly secured servers or storage media, the hacking of systems and retention of copies of data by contractors temporarily authorized to possess the data for service-related purposes. Data leakage magnifies the risk of misuse, including through inappropriate publication of damaging information.

DATA RETENTION

The information technology phenomena that are driving development of data mining techniques also enhance the likelihood that personal information fed into and derived from data mining projects will linger for longer and longer. Data storage is becoming cheaper every day and the technologies to find and exploit archived data are advancing all the time. These factors will be partly responsible for creation of the digital personality—the digital construct of each of us that will, in important ways, mediate between our true selves and the rest of the world, notably government.

What makes the description of a person in today's global data world especially worrisome is that the portrait created is not a portrait of one's true self. Our digital selves, in other words, can hardly reflect our true selves. Analysis of data can create a caricature, but it does not create a person—and the essence of privacy is maintaining your personhood. This is of more than philosophical concern. The pooling of data streams and analysis of the data can have real and costly consequences for individuals. The longer these data linger, the harder it is to correct errors or to ensure currency, particularly where the information system is a secret national security system. Even where the data are accurate, their permanent retention will raise serious problems for those who might wish, and deserve, to be able to move on with their lives. It will become more and more difficult to obscure the folly, for example, of a youthful flirtation with radical politics. Aware of the power of our digital personae, we may withdraw or tend to the anodyne. This is hardly conducive to individual fulfillment or the wellbeing of society and government.



FALSE POSITIVES

An example offered in the very country, where it all begun, the US, media reported last year the Senator Ted Kennedy was told he could not board more than one domestic flight because the name T. Kennedy was on the US no-fly list, CAPPS I. His name generated a hit when run against the list, so he was banned from flying. These were false positives—he was not the T. Kennedy on the list and should not have been flagged as a security risk, even if the ‘real’ T. Kennedy should have been. Senator Kennedy ultimately caught his flights because he was able to persuade managers on the scene that he was not a risk. Someone not as well known might not be so fortunate. A number of examples have been reported where individuals have been kept off flights in the US due to false positives. This is more than a minor hassle for those unable to visit an ailing parent or attend a loved one’s funeral. This is more than merely inconvenient for those who must fly on business. If they cannot travel when required, their jobs are in real jeopardy (and it will certainly not help an employee if the employer discovers that the employee cannot fly because she or he is on a terrorist no-fly list).

The problem of false positives is not unique to data mining, but our tendency to trust data and the scope for significant numbers of false positives promise, in combination, to make this a pressing issue. The risk of false positives is a system-design issue. If a data mining application cannot distinguish the ‘noise’ of ordinary behaviour from signs of possible terrorist activity, individuals will falsely be singled out for investigation or wrongly be put on watch lists. This is not to say that data mining should never be used for terrorism-related work. Rather, effective technological solutions must be found, and meaningful procedural and substantive protections must be implemented, to guard against the impact of false positives.

FUNCTION CREEP

It is an axiom of privacy that personal information gathered for one purpose will inevitably find other uses: Once the systems to access and use personal data are in place, there is an understandable interest in using those systems for other worthwhile purposes (e.g., preventing and prosecuting violent crimes). The consistent experience with data protection suggests that, over time, there is



always pressure to use data collected for one purpose for other purposes. The expansive uses to which Social Security Numbers have been put are a practical example.

In the context of data mining for national security purposes, information generated for investigative purposes, or for use on a no-fly list, might be used for ordinary law enforcement purposes or to blacklist individuals.

BLACKLISTING

Terrorist watch-lists are being used in one form or another in some countries. Watch lists can have legitimate, even important, functions. Use of watch lists ought, however, to be confined to a limited scope of functions such as terrorism investigation, intelligence-gathering and security clearances. A watch list could turn into a blacklist—a list used as secret evidence, or effectively as a secret finding, to make decisions that directly affect individuals who have no knowledge of the evidence or any ability to challenge it. Blacklists can, of course, be officially sanctioned or illicit. In either case, they are a concern, one that is magnified given the risks such as poor data quality that can be associated with data mining.

WRONGFUL MISUSE OF DATA

Concern about misuse of information derived from data mining activities is by no means unique to data mining. Examples abound from other areas, both in the public sector and the private sector. Embarrassing or lucrative personal information tempts intentional misuse and the products of data mining will also be tempting.

LACK OF DUE PROCESS

Experience with national security data mining initiatives, suggests that authorities can be slow to recognize the need for due process and other protections. It appears, for example, that the Transportation Security Administration has been slow to devise due process protections for those



who find themselves incorrectly placed on no-fly lists in the US. Yet it is critically important that individuals mistakenly placed on no-fly lists or otherwise affected by errors or abuses of data mining systems be able to obtain redress through independent, fair, simple and as transparent as possible oversight processes.

DATA MINING & PRIVACY LAWS

There is a body of internationally-accepted fair information principles that are reflected in privacy laws throughout the world and in international instruments and that can be used as a foundation of privacy laws. Such laws aim to give individuals a degree of control over their own personal information throughout its life cycle. They give individuals the right to be told what information is being collected about them, who is collecting it, the uses to which it will be put, to whom it might be disclosed, and for what purposes it might be disclosed. In the private sector, the rules aim to give individuals a further degree of control by enabling them to generally choose which information to give up and for what purposes. Privacy laws also give individuals the right to have access to their own information. They require organizations to take reasonable steps to ensure that personal information they hold and use is accurate and complete.

However, many of these rules are not fully equal to the task of meaningfully protecting privacy against risks associated with data aggregation, data sharing and data mining for national security purposes. The power of these information technologies, and the risks to individuals and society, are such that new approaches to privacy protection are required to supplement existing ones.

KNOWLEDGE OF COLLECTION

An axiom of privacy protection is that, with limited exceptions, individuals must be given notice of collection of their personal information at the time it is collected. As indicated earlier, data mining almost invariably depends on collection of personal information from a variety of sources and, certainly in the national security context, this means affected individuals will usually not know of the collection of their personal information. Some observers might suggest that this could be



addressed by requiring information sellers or providers to notify affected individuals of the government's collection of information. This will be of questionable efficacy even where it is feasible at the time of collection. Further, such an indirect notice requirement is unlikely to work where personal information is collected for national security purposes, since notification will be dispensed with where national security is involved.

NOTICE OF THE PURPOSES FOR COLLECTION

Another important privacy principle is that individuals are to be told the purpose for which their personal information is collected. The original collector of the information will not be collecting it for a national security purpose. This principle will therefore be honoured in the breach when the information is acquired later for national security uses.

DIRECT COLLECTION

Privacy laws stipulate that personal information can only be collected directly from the individual the information is about. There are exceptions to this, including for ordinary law enforcement needs—police can hardly be expected to ask a suspect for personal information needed to prosecute the suspect. The same will hold true for national security activities, meaning that indirect collection for national security data mining uses will be the norm, not the exception.

LIMITED COLLECTION

Although the precise standards vary somewhat, some privacy laws permit organizations to collect only the personal information that is necessary for, or relevant to, the purpose for which it is collected. Where an individual's personal information that is initially collected for a commercial purpose is later used for national security data mining in conjunction with other information, the limited collection principle may have little meaning and offer inadequate protection.



INDIVIDUAL ACCESS

An important privacy right is the right to have access to one's own personal information. This enables individuals to find out what personal information an organization has about them, how it has been used and to whom it has been disclosed. It goes almost without saying that this right is illusory in the national security context.

ACCURACY AND COMPLETENESS

Privacy laws require organizations to take reasonable measures to ensure that personal information they use to make a decision affecting an individual is accurate and complete. This is not a counsel of perfection, of course, but it does require positive, ongoing efforts to ensure data quality and completeness. Unlike the other traditional rules just mentioned, this duty is meaningful in the data mining context. It is necessarily imprecise and sensibly technology-neutral, but it can be particularized on an evergreen basis at a policy and operational level. A lingering concern, however, is whether meaningful independent oversight of the design of, and compliance with, this duty is available under the present privacy protection scheme.

INDEPENDENT OVERSIGHT

As with any rights, rights to privacy mean little unless they can be vindicated through the rule of law. Independent oversight is a central tenet of internationally accepted privacy principles. Numerous privacy laws provide for independent review and (to varying degrees) enforcement of privacy rights through commissioners or Ombudsmen with privacy oversight duties.

PRIVACY MEASURES FOR DATA MINING

As the preceding discussion shows, privacy risks associated with data mining present challenges that our existing privacy laws are in large measure ill-equipped to meet. This is not to say that privacy laws are irrelevant in the context of data mining and other information technologies



deployed for national security purposes. To be sure, the long-standing principles of limited (and proportional) collection of personal information, use of personal information for the purpose for which it was originally collected (or a very closely related purpose), information security and independent oversight remain relevant in the context of these new technologies.

While no single approach can adequately address all risks, solutions can and must be found. There is a pressing need for governments, to study the available options and move quickly to implement effective and workable legal, policy and technological measures to protect privacy. Some, but not all, of the more significant measures worth considering are now outlined. Taken together, they can to some degree meet the pressing need for legislative and policy reform that provides for a comprehensive, one-stop approach to data mining approval and regulation for national security purposes.

DATA MINING RESEARCH

Before federal government agencies engage in data mining the federal government should undertake research into the effectiveness of data mining, with emphasis on technological and other tools for enhancing privacy protection. The research should also consider legal, social and ethical issues associated with data mining.

To be clear, a central focus of this research should be whether data mining for national security purposes offers meaningful benefits that are sufficiently important to override privacy and other civil rights concerns. It was acknowledged above that data mining can be useful for national security purposes, but before any data mining initiatives proceed it is necessary to establish that any such benefits clearly and substantially outweigh the risks for privacy and other rights and liberties and that any such risks can be properly mitigated. This is not merely an exercise in assessing the constitutionality of proposals. It is a question of responsible and proportional policy making. Data mining should not be used for national security purposes unless stringent conditions are met.



PRIVACY IMPACT ASSESSMENTS

A privacy impact assessment is a process -and an ongoing one at that- that requires an organization to assess the privacy risks of proposed programs, systems or laws and, to decide, whether they should proceed and to identify and implement mitigating measures where they do proceed. A PIA process enables privacy to be designed into new systems from the outset, thus promoting efficiency as well as good privacy practice and compliance. A mandatory PIA process, ideally with sign-off by the external oversight agency, should be a mandatory feature of any data mining governance framework.

CHIEF PRIVACY OFFICERS FOR NATIONAL SECURITY AGENCIES

Large corporations now commonly have a chief privacy officer (“CPO”) responsible for privacy compliance and oversight within the organization. These positions are often at the senior executive level, which recognizes the importance to a corporation’s brand of good privacy practices and compliance.

At the very least, agencies involved in national security and anti-terrorism activities should establish well-resourced, executive-level, CPO positions with responsibility for ensuring that information technologies such as data mining are designed and operated lawfully. It is time such positions were created, with executive support and real internal authority.

PRIOR JUDICIAL AUTHORIZATION FOR DATA MINING ACTIVITIES

There should be a strong rule that data mining can be performed only on anonymized data, with identification of individuals being possible only when specified quality and cogency criteria have been met and then only with prior judicial authorization. The technology exists to do this. This rule would be relevant particularly in relation to data mining undertaken at a population or large group level. Where data mining is proposed in relation to specified individuals, it should be permitted only with prior judicial authorization on the basis of particularized grounds that meet constitutional standards.



RULES-BASED AND OTHER TECHNOLOGICAL PROTECTION

A number of technical approaches to data mining are available to enhance privacy in data mining, while more research is required to refine other techniques before they can credibly be deployed. Rules-based processing techniques, it has been said, offer considerable promise for privacy protection in data mining. One technique would involve use of intelligent agents (or “proof-carrying code”) to centrally query distributed databases by negotiating access and permitted uses on a database-by-database basis. Where data elements might move about, they could be labelled with meta-data stipulating how the element must be dealt with. This technique would allow rules specific to particular data elements to follow the data elements. A third approach involves software applications known as ‘analytical filters’, which are designed to filter and discard innocent noise and retain information of interest.

AUDIT TRAILS

Information systems in health care and commercial applications are now commonly equipped with built-in audit systems. The best of these systems automatically log access to data files and create more or less immutable audit trails. At the most basic level, they can in real time identify when unauthorized access is attempted or succeeds. More sophisticated audit applications monitor authorized access for unusual patterns and can, either automatically or with human intervention, identify both inappropriate access and use by authorized users. These systems enable administrators (and regulators) to ensure that rules are followed. In the context of sophisticated and powerful information technology like data mining, strong audit capabilities are of critical importance in preventing misuses of data, data spills and even function creep.

SECURITY OF DATA MINING SYSTEMS

Although a trite proposition, data mining systems must have strong security measures in order to prevent data leakages or corruption. As noted earlier, one generally-accepted privacy principle



that applies to data mining in a meaningful way is the obligation to take reasonable security measures to protect personal information against unauthorized collection, use or disclosure. This is especially important in light of the risks that can be associated with data mining by the state. Data security must be a high priority in the design and operation of data mining systems.

DUE PROCESS FOR AFFECTED INDIVIDUALS

As mentioned earlier, the fact that national security is involved cannot be allowed to oust due process for affected individuals. If someone is incorrectly placed on a watch list or no-fly list, or is investigated on false premises, they should have recourse to an effective process for redress. The process should, despite the national security nature of the enterprise, be as transparent as practicable in the circumstances, should be inexpensive, and should be expeditious.

ENSURING EFFECTIVE EXTERNAL OVERSIGHT

Last, but by no means least, some way must be found of ensuring that there is effective, independent, oversight of data mining activities. The rights and freedoms that we have come to expect, including our privacy rights, are not absolute. Terrorism may necessitate new strategies to protect the security of all people. Although the risk of terrorist attacks is real, governments must take great care not to overstep the line. Although it may be true that, the more freedom people have, the greater the potential risks are.

Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known. Privacy can be seen as an aspect of security—one in which trade-offs between the interests of one group and another can become particularly clear.

The right against unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries' laws, and in some cases, constitutions or privacy laws. Almost all countries have laws which in some way limit privacy, for example taxation normally requires



passing on information about earnings. In some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures.

Privacy may be voluntarily sacrificed, normally in exchange for perceived benefits, but often with little benefit and very often with specific dangers and losses. An example of voluntary sacrifice is entering a sweepstakes or competitions. A person gives personal details (often for advertising purposes) in order to have a chance of winning a prize. Another example is where information voluntarily shared is later stolen or misused such as in identity theft.

Reasons for maintaining privacy

If "information is power", then it follows that personal information in whatever form, or of whatever nature, confers power to the owner of that information. Few individuals, organizations or governments refrain from making judgements based on their own self interest and the information gained through the loss of privacy, tends towards ultimately being used to wrestle power and autonomy away from the individual. The loss of privacy in a modern and evolving technological age, risks putting intolerable strains on existing democracies, by empowering governments beyond their ability to contain their natural inclinations towards totalitarian actions and recurring dictatorial political forms.

Until the corrosive effects of power on the human psyche can be understood and sympathetically managed, it seems likely that increasing losses of privacy will inevitably lead to corresponding loss of personal freedom, if only through the psychological effects on the individual, from the perception that they are being continuously and relentlessly scrutinized. This has been referred to as a 'technique of mass submission'.

The political effects of sustained and expanding losses of privacy also risk the eventual perception that even the secret ballot of the democratic vote is compromised. In an increasingly paranoid and totalitarian state this becomes a relevant factor. Also see Totalitarian democracy.

It has been reasoned that privacy encourages information sharing between individuals, because



it creates an environment in which any perpetuated information that does not reference a source can be identified as rumor. If information is shared voluntarily, then facts can generally be approved by references to one or several identified sources, and there are fewer chances for the perpetuation of mistrust. The reasoning behind this is that the intention of a privacy violation does not matter for its effect to perpetuate the environment of rumors that is the root cause of intolerance. Philosophers often ask how people can choose to trust each other if they cannot hide from each other.

One may also wish to maintain privacy by withholding information from others because of stigma (as in the case of some "closeted" homosexuals), or for protection from the law (as when criminals hide information to prevent others from catching them). Often, information (such as bank account numbers or, in the USA, the Social Security Number) may be used against the owner of the information, for example to commit fraud. By maintaining privacy, information owners hope to avoid this fraud or limit effects from it.

Reasons for not maintaining privacy

It has been reasoned that privacy discourages information sharing between individuals which in turn can lead to mistrust and intolerance amongst people and perpetuate false information. If information can be shared widely then facts can generally be verified through many different sources and there are less chances of inaccuracies. It has also been reasoned that Privacy can perpetuate stigma and intolerance. The reasoning behind this is that restrictions on information about people can inhibit and discourage collection and finding of data that is required for an accurate analysis and discussion on the causes and root of the stigma and intolerance. Philosophers often ask how people can learn to accept each other if they cannot know about each other. Issues have also been raised that privacy can encourage criminal activity as it makes it easier for criminals to hide their unlawful activities.

More pragmatically, privacy sometimes is not maintained because there is a benefit provided by disclosure. For example, a potential employer is given a résumé/CV in order to evaluate someone's appropriateness for employment. Or, contact information, e-mail addresses most often, are provided in exchange for access to some useful information, like a "white paper".



INTERNET PRIVACY

Using the Internet leaves a trail of information about one's activity if privacy software, careful clean-up or a proxy server is not used. A user's computer can reveal, for example, a web browser's history, cache or logs to reveal what the user has done. Websites will also have their own logs showing the IP address and other demographic data from each computer to which it provides access.

An additional Internet privacy concern involves the erosion of “security through obscurity” as web search engines provide increased access to personal information online, such as public records, social networking profiles, biographical webpages or online resumes.

Arguments for government monitoring

- Increased crime detection - due to the placement of CCTV cameras, the success rate of conviction is increased as criminals are more likely to be convicted due to the increased ability to prove a suspect committed an offence.
- Prevention of terrorism - terrorist activities need coordination and this is often done using electronic equipment. If communications between devices can be monitored, the activities of terrorists can be prevented before any terrorist attacks are carried out, and their networks can be disclosed by network analysis and traffic analysis.

Arguments against government monitoring

- Surveillance infringes on civil liberties - there is a lack of anonymity if facial recognition systems can be used, for example, to identify protestors in a demonstration.
- CCTV cameras displace crime, rather than eliminate it - criminals move to areas where CCTV is not in place.
- Due to the enormous manpower require to operate and monitor, many crimes (even if recorded) go unnoticed for hours, days, or even months, while costing money for upkeep



and wages.

- Monitoring can be used in committing crime, for example police officers have been caught using cameras to invade the personal privacy of women walking through airports.
- Gathering data about many people in one place (the monitoring centre) provides a valuable source of data which would fuel illegal activities if the integrity of the operators were ever compromised.
- The same technology used for disclosing networks of terrorists and criminals can be used by repressive regimes for finding dissidents, and allows easy blackmailing, blacklisting or prosecuting of people for their guilt by association (see the Second Red Scare for a set of historical examples). Its presence itself can provide a considerable chilling effect for political dissent.
- An increase in methods to track individuals and their movements could create a large distrust in the government.

Telecommunication is the transmission of signals over a distance for the purpose of communication. In modern times, this process almost always involves the sending of electromagnetic waves by electronic transmitters but in earlier years it may have involved the use of smoke signals, drums or semaphore. Today, telecommunication is widespread and devices that assist the process, such as the television, radio and telephone, are common in many parts of the world. There is also a vast array of networks that connect these devices, including computer networks, public telephone networks, radio networks and television networks. Computer communication across the Internet, such as e-mail and instant messaging, is just one of many examples of telecommunication.

Society and telecommunication

Telecommunication is an important part of many modern societies. In 2006, estimates place the telecommunication industry's revenue at \$1.2 trillion or just under 3% of the gross world product.



Good telecommunication infrastructure is widely acknowledged as important for economic success in the modern world on a both micro- and macroeconomic scale.

On the microeconomic scale, companies have used telecommunication to help build global empires. Even relatively poor communities have been noted to use telecommunication to their advantage. From any perspective the economic benefits of good telecommunication infrastructure are undeniable and, for this reason, there is increasing worry about the digital divide.

This stems from the fact that access to telecommunication systems is not equally shared amongst the world's population. A 2003 survey by the International Telecommunication Union (ITU) revealed that roughly one-third of countries have less than 1 mobile subscription for every 20 people and one-third of countries have less than 1 fixed line subscription for every 20 people. In terms of Internet access, roughly half of countries have less than 1 in 20 people with Internet access. From this information, as well as educational data, the ITU was able to compile a Digital Access Index that measures the overall ability of citizens to access and use information and communication technologies. Using this measure, countries such as Sweden, Denmark and Iceland receive the highest ranking while African countries such as Niger, Burkina Faso and Mali receive the lowest.

In a world where literally everything you do can leave a digital fingerprint, it is only a question of how willing various data collectors are in maintaining the privacy of users. The potential for abuse is enormous.

We all want sensitive personal and financial data to be secure from theft and misuse. But the issue of privacy is more than security alone. There are complex questions of who controls the data about us (individually and collectively) and how it is used.

The European Union's Directive on Data Privacy enacted in 1998 is a case in point. The law prohibits the transfer of personal data to non-European Union nations that do not meet its guidelines for privacy protection. The Directive provides for the creation of government data protection agencies that will oversee the registration, and in some cases the approval, of databases containing personal information.

There are 30 or so federal statutes and over 100 state statutes governing information privacy in the U.S. The approach has been piecemeal in protecting privacy. It blends government oversight



with industry self-regulation, and varies from sector to sector. Because of this, companies doing business over the Web with consumers residing in the E.U. can find themselves in non-compliance with the local requirements for privacy protection. To help companies comply with the E.U. regulations the Department of Commerce has developed a set of rules under which U.S. businesses should operate, called the safe harbor principles.

Privacy is the right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others. Framework

CURRENT ENVIRONMENT

As business systems and processes become increasingly complex and sophisticated, growing amounts of personal information are being collected. As a result, personal information may be exposed to a variety of vulnerabilities, including loss, misuse, and unauthorized access and disclosure. Those vulnerabilities raise concerns for organizations, the government, and the public in general.

Maintaining the privacy and protection of customers' and employees' personal information is a risk management issue for all organizations. The increase in identity theft is a concern for all organizations. Laws and regulations continue to place requirements on businesses for the protection of personal information.

Individual states have also asserted their prerogatives in the absence of certain national privacy laws. For example, an issue active for several years and vastly accelerated in 2005 is regulation by states when data security breaches involve personal information. States are continuing to enact new laws in this arena.

Generally Accepted Privacy Principles (GAPP) have been developed from a business perspective, referencing significant domestic and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that need to be met. Illustrative policy requirements, communications, and controls, including monitoring controls, are



provided as support for the criteria.

WHAT IS PRIVACY?

Under GAPP, *privacy* is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

PERSONAL INFORMATION

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are:

- Name
- Home or e-mail address
- Identification number (that is, a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions



Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, the use of sensitive information may require explicit consent rather than implicit consent.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as nonpersonal information. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains, because the information is de-identified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual.

PRIVACY OR CONFIDENTIALITY?

Unlike personally identifiable information, which is often defined by regulation in a number of countries worldwide, there is no single definition of confidential information that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires to be maintained on a need to know basis. Examples of the kinds of information that may be subject to a confidentiality requirement include:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its



accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organization to organization and in most cases are driven by contractual arrangements.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. Governments are trying to protect the public interest but, at the same time, manage their cache of personal information gathered from citizens. Consumers are very concerned about their personal information and many believe they have lost control of it. Furthermore, the public has a significant concern about identity theft and inappropriate access of personal information, especially financial and medical records. Domestically and internationally, a patchwork of laws and regulations is being debated to address the fears, the realities, and projections of future challenges.

Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy.

GENERALLY ACCEPTED PRIVACY PRINCIPLES

Generally Accepted Privacy Principles as developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA) form a comprehensive resource providing guidance on a number of areas related to privacy. Privacy and security practices for personal information, organized into 10 principles.

The following are the 10 Generally Accepted Privacy Principles:

1. **Management.** The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.



3. **Choice and Consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use and Retention.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to Third Parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for Privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and Enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

The Universal Declaration of Human Rights, in article 12, states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.



We can find in many countries (such as France) rules that protect privacy explicitly (such as France in the constitution -France's Declaration of the Rights of Man and of the Citizen, the Supreme Court of the United States has found that the U.S. constitution contains "penumbras" that implicitly grant a right to privacy against government intrusion). Other countries without constitutional privacy protections have laws protecting privacy, such as the United Kingdom's Data Protection Act 1998 or Australia's Privacy Act 1988. The European Union requires all member states to legislate to ensure that citizens have a right to privacy, through directives.

Bodies and organizations

- American Civil Liberties Union (ACLU)
- Electronic Frontier Foundation (EFF)
- Electronic Privacy Information Center (EPIC)
- Privacy International
- Data privacy
- Data retention
- Secure communication
- Generally Accepted Privacy Principles
- Privacy Commission Privacy Watch Review (and other resources)
- Electronic Frontier Foundation digital rights NGO
- Electronic Privacy Information Center a public interest research center
- Privacy International UK-based International privacy NGO
- Privacy Spot privacy law blog
- The Privacy Place Research Center
- OECD Guidelines on the Protection of Privacy describe principles behind many contemporary privacy laws
- Data Protection in the European Union, from the Directorate-General for Justice, Freedom and Security

Every increase in security almost inevitably curtails rights and freedoms that are at the heart of democratic societies. Rights and freedoms that we tend to take for granted because we have always been fortunate enough to have them can be easily eroded—in good faith or otherwise—and we must



ensure that our elected officials maintain life and vibrancy in them.

No one can envy the difficult task lawmakers face in trying to strike the right balance between privacy and security, but it is critically important that they ask the hard questions and come up with appropriate answers. Meaningful reforms of privacy laws are urgently required in order to address the privacy challenges raised by data mining and other information technology applications. Those reforms are needed now.