Privacy Issues and Privacy Enhancing Technologies

by Lauren Weinstein and Peter G. Neumann
15 February 2003

Addition *by Cameo Wood*

Contact: *Lauren Weinstein*
lauren@pfir.org
Peter G. Neumann
neumann@pfir.org
Cameo Wood
cameo@kiad.net

Contents

Abstract

This report considers the state of privacy issues and major sources of privacy problems in the United States (and related international issues), summarizes the most important potential privacy-enhancing technologies, and illustrates the major risks through cases of serious violations of privacy that have been reported. It also considers the sorts of problems that should be expected in the near future if current anti-privacy trends continue. Most of these issues will be applicable on an international basis, and may be of serious concern in Japan.

Introduction and Executive Summary

Privacy is a concept with many different meanings to people and cultures around the world. To some persons, it means the freedom to be "left alone" so long as their activities don't impinge upon the rights of others. Privacy can also connote protection of information from misuse or abuse, especially when that information is stored in computers and transmitted through communications media.

While persons living in small towns one hundred years might have had little expectation of privacy in the sense we think of it today (after all, everybody knew what everyone else was doing then!) in our modern societies an expectation of greater privacy has arisen along with the rise of our technological prowess — at least until relatively recently.

The ability of modern computers, databases, and telecommunications systems to integrate and "data-mine" personal data in ways unimaginable even ten or twenty years ago is vast, and bring with it enormous opportunities for abuse and misuse.

Making matters worse, the legal and judicial systems in most countries have not kept pace with these developments, perpetually being in a state of playing "catch up" to fix privacy abuses after they've occurred, rather than taking a proactive stance that might have protected the privacy of its citizens and other residents in the first place. Often by the time such corrective actions are taken (to whatever extent those actions exist), the personal data involved may already be widely abused; no practical means exist to "take back" that data and protect it again retroactively. Personal data once revealed is usually revealed effectively forever.

Powerful interests in government and business are also responsible for making the privacy situation worse. Governments may use security concerns as an excuse for anti-privacy actions that do little to increase real security (however, useful and laudable they may ostensibly appear from a public relations and political standpoint) but that actually merely crush civil liberties and move toward a police state society.

Traditionally, public-record information such as birth, death, court, and a wide range of other government records becomes the fodder for massive abuse (on the part of both the public and private sectors) when it becomes easily accessible en masse through database systems, sometimes even being treated as a profit center by government agencies. The same information that was relatively harmless on index cards in a card file (which required significant effort to research and obtain) becomes qualitatively changed by the kind of access that computers and databases provide to the data. Furthermore, the potential for resulting problems is gigantic.

Businesses tend to treat the personal information of their customers as a mere commodity — like potatoes or hog bellies — to be traded, sold, and exploited massively with no real control (or even knowledge of these actions) on the part of the customers themselves whose data is being manipulated and often abused in these ways.

In the United States, a confused hodgepodge of conflicting laws and regulations at the federal, state, and local levels has created an terrible mess when it comes to privacy issues. Businesses pretty much run the show, with little real concern about consumer rights beyond that absolutely necessary to meet the weak and limited government regulations that exist in specific areas like the credit and financial services sectors. Large portions of the most privacy-invasive aspects of business, including the Internet, are still largely unregulated and privacy abuses have been rising in all of these areas at an extremely alarming rate.

The U.S. provides in some respects an excellent negative example — namely, how not to deal with privacy concerns — at least in comparison with some countries (such as those of the European Economic Community). That's not to say that the EEC has done everything right in this regard. Some of their (especially recent) actions regarding privacy and surveillance are extremely negative themselves. However, the EEC has at least started down the path to defining privacy issues in a systematic and broadly applicable manner, a path the U.S. stubbornly refuses to really consider.

In the wake of the terrorist attacks of September 11, 2001, and the U.S.'s new infatuation with preemptive war as a global "stabilization" technique, many entities with highly anti-privacy agendas have seen new life in their old proposals. Formerly unable to get their draconian agendas enacted into law, they're now seeing success in exploiting the "war

on terror" as an excuse for enacting all manner of anti-civil-liberties and anti-privacy measures, most of which will not actually fight terrorism in any significant way.

It's a bad time for privacy.

Most people never really even consciously think about privacy matters to begin with until their privacy has been eroded, and that loss usually occurs little by little over a long period of time, with potentially devastating results.

Protecting privacy takes a great deal of diligence, work, dedication, and perseverance, especially in the face of increased computerization, cross-linking of information databases, dependence on the Internet, and ever-growing efforts to misuse existing and new information and data for both public and private-sector purposes.

Many of these related problems are discussed in this report, including difficulties associated with personal identities, computer databases, and many related issues. In addition to identifying the areas of concern, we have endeavored to note the roles that technology could play in helping protect privacy, assuming an environment that permitted and encouraged their use. We have also included various examples of privacy problems and related risks that have occurred in the past, in the hope that these may be of assistance in illustrating the risks that are now faced by individuals, organizations, and even governments today and in the near future.

A glossary of specialized definitions used in this report is provided as an appendix. These terms relate to identities, authentication, authorization, accountability, anonymity, pseudoanonymity, and other associated areas.

Since this report is of necessity limited in length, it can only cover these complex topics relatively briefly. We most strongly urge the interested reader to refer to the various references we have included for additional information on particular topics and detailed facets of these critical privacy issues.

SSNs and Other Identification Schemes

In the United States, the Social Security Number or SSN plays an important yet rather paradoxical role. While nearly all persons in United States earning income are required to possess a Social Security number, the Social Security card that lists the number is itself not an identification card. In fact, historically the Social Security card has been specifically labeled that it is not to be used for identification purposes. While a person may be asked for their Social Security number in a wide range of contexts, they will very rarely be required to display the actual card.

The ostensible purpose of the SSN is to provide a means to record and track a person's financial activity, particularly for tax purposes. Virtually all of a persons' federal and state income tax and other tax liabilities and records, are indexed by the nine-digit SSN.

The name "Social Security" relates to the fact that the number was originally created to facilitate not only the collection of taxes but also the distribution of all old-age and other related benefits that are part of the Social Security system.

However, in the decades since the Social Security Number's appearance, the SSN has gradually become used as a universal identifier for all manner of transactions, many of which have absolutely nothing to do with taxes or other government activities. This has led to the Social Security number being abused widely and becoming a primary factor in the spread of identity fraud which has now reached astronomic proportions.

Because the Social Security number is not generally considered to be confidential information (particularly as a result of relatively recent court actions) a vast array of non-governmental organizations, businesses, and even individuals, use the Social Security number to provide a means for both record-keeping and investigatory purposes whether legitimate or not. Not only does the U.S. Social Security card not include any form of biometric identification, it does not even include a photograph, further emphasizing the fact that it is not actually an identification card of any kind.

Due to lax controls over the purposes to which the SSN can be put and the ways in which it can be transferred between parties, the SSN has now become a de facto standard for indexing important consumer records such as health insurance, credit card transactions, credit records of all types, and a vast range of other information. In some areas, the Social Security Number has even been used as a reference for such purposes as library cards and school student identification numbers. Obviously, the use of SSN for such purposes opens a tremendous amount of risk. For example, a students' ID card would typically be used for a wide range of transactions and would be accessible to many persons in the course of routine activities.

Since that same number is so widely used for other purposes, once it has been obtained it becomes fodder for wide abuse. To make matters worse, many credit card companies, banks, and other institutions, use the Social Security Number as a customer password for obtaining information or conducting transactions by phone. Also frequently used is mother's maiden name and date of birth. Individuals' SSN

information, date of birth, and mother's maiden name have become easily accessible in many cases through public record databases.

In some states, the Social Security Number has even been displayed on drivers' licenses — which are the predominant form of identification card in the U.S.. While recent changes in the laws have introduced some minimal safeguards relating to the disclosure of SSN in the context of driver's licenses, the opportunity for abuse is still very broad. For example, until a few years ago, the U.S. Internal Revenue Service was routinely making SSNs visible as part of the address information on postal service mailings to taxpayers.

Driver's Licenses and State-issued "Identification" Cards

Without a doubt, the primary form of identification used by most persons in the United States is the driver's license. Each state has its own rules for issuing drivers licenses or in the case of non-drivers state-issued "identification" cards,.

In the vast majority of states, these cards include a photograph of the individual. Even when it is not present on the driver's license, most states now require the submission of the applicant's Social Security number to be associated with their state records. The original rationale for the Social Security number requirements relating to drivers licenses was to help in the search for "deadbeat dads" who were not paying child support payments. However, new federal laws have mandated the wider availability and use of SSN and data relating to these cards.

Recent federal legislation also has moved toward harmonizing the information required to be collected by all states. It is widely assumed that moves toward additional forms of biometric identification for these cards, will be mandated. At the present time, the usual biometric information included on the cards and in individuals records in most states is typically a single thumbprint.

Moves toward the use "smart cards" will undoubtedly encourage officials toward requirements that additional machine-readable information be included within these cards.

It has therefore become an issue of great concern that these sorts of moves and developments relating to drivers licenses will result in the creation of a de facto national ID card in United States that could ultimately be required for all manner of transactions or movements, even though the cards themselves would be issued by the states and would be supposedly be nominally under state control.

Drivers licenses and state issued identification cards for non- drivers as mentioned above, are theoretically voluntary at this time. In practice, a wide range of transactions are impossible or difficult to engage in without one or the other. Many merchants now wish to see a customer's drivers license before accepting a credit card or check.

While few merchants currently have the technical means to scan and collect information off of the limited capability magnetic stripes on most current generation drivers licenses, advances in technology will no doubt make critical the issues both of what information is stored on the cards (either visibly or invisibly on magstripes or internal chips) and who will have the capability and authorization to read, collect, store, and use that data.

Spread, Control, and Abuse of Collected Data ("Data Creep")

A fundamental problem relating to privacy issues both in United States and elsewhere around the world, relates to the problem of "data creep." This describes the phenomenon where information that is collected legitimately for one purpose becomes available either legitimately or illicitly, for a range of other often unrelated purposes.

This sort of leakage of personal information is at the heart of many privacy-related problems. While some countries (particularly in the European Union and Canada) have taken steps or passed laws aimed at controlling this sort of information flow, the United States in general has been lagging far behind. The U.S. does not have anyone who could be equated to a national privacy ombudsman or "czar" covering all aspects of U.S. residents' privacy concerns. For example, while recent legislation ostensibly created some new information privacy requirements for financial institutions, in practice these are considered extremely minimal and far from adequate.

Attempts to require financial institutions to operate on an opt-in basis — that is, not sharing information about consumers without their explicit permission beforehand, have been generally unsuccessful. Instead, laws generally have allowed an opt-out approach, where it is assumed that information can be shared unless a person explicitly says otherwise.

In practice, this is basically a giveaway to businesses, since few consumer really understand what information about them has been collected and how it could be used or abused, and so few realize that they should take positive steps to exercise their opt-out privileges even where these do exist.

Matters are made even worse by the manner in which

institutions and businesses usually notify customers about these privacy issues. Online privacy policies (e.g. on the Web) tend to be on unobvious in many cases and often are written in complex legal language that fews users would understand, even if they had time to read the often extremely lengthy texts. Even worse, such online privacy policies are subject to change anytime, usually without any explicit notification to consumers that changes have occurred.

Laws that have mandated inclusion of privacy information and opt-out information in bills and other mailings to consumers have had little positive effect. These inserts are usually in the form of small brochures with tiny print written in complex terms, and are easily confused with a multitude of other literature and advertising that often stuffs these mailings and are typically discarded unread by many recipients. Sometimes the mechanism provided for exercising opt-out privileges is also cumbersome, e.g. requiring a written letter rather than a call to a toll-free telephone number. It is also usually the case that there is no clear-cut mechanism to verify that an opt-out has actually been properly processed within these systems.

The vast amount of personal information, advertising, and other data that is collected and used, makes it utterly impossible for consumers to determine the actual status of their information in the multitude of governmental and commercial databases that exist. There are no requirements for standardized methods for interrogating most of these databases, with the exception of the major credit reporting agencies which collect individuals' credit history, credit worthiness, and other related information, and which have been themselves the subject of specific legislation relating to access to information and mechanisms for submitting complaints or corrections to such data. (See the section on illustrative risks cases, below.)

Another aspect of the situation, that makes attempts at opt-outs and other consumer control over their personal information so difficult, is that the laws relating to this area usually exclude from controls the sharing of information between organizations that are part of the same corporate entity or in some cases are closely allied. With the vast expansion of gigantic corporate mergers, especially mergers between different sorts of financial institutions, this exception alone opens up an enormous possibility for personal information sharing that falls outside the limited controls of existing privacy-related laws.

Collection, Use, and Abuse of Telephone-related Data

Another area of concern in the U.S. relates to the use of customer information (such as Customer Proprietary Network Information — CPNI) by communications-related firms such as telephone companies. This information can be shared and exploited in a number of situations under current law. It relates to consumers' communications use including calling patterns, billing information, and other related data.

As with some other forms of consumer information that we discuss, there are some opt-out availabilities for some of this data, but since few consumers understand these issues few avail themselves of the opportunities to protect this information. Recent attempts to tighten down on this area and provide further limits to telephone company use of such data have recently been unsuccessful, resulting in the likelihood of further battles and controversy in this area.

Effects of Post-September-11 Laws on Privacy Issues

Many aspects of U.S. laws — at federal, state, and local levels, have been thrown into question or affected in various ways by the terror attacks on September 11, 2001. Legislation resulting from those attacks, including the USA Patriot Act and the Homeland Security Act have called into question much of the progress that had been made before this time relating to privacy matters, however minimal that progress might have been up to that time.

It has also very recently come to light that the U.S. Justice Department is considering requesting from Congress a range of additional domestic security law changes that could have additional anti-privacy effects.

The USA Patriot Act and Homeland Security Act allow for a vast range of privacy-invasive activities by government and in some cases by private firms, ostensibly to help fight terrorism. However, these laws were drafted and enacted very quickly, in a knee-jerk fashion, and were not limited in most cases to anti-terrorism efforts. These laws and other like them will have drastic impacts across a wide range of non-terror-related law enforcement activities including monitoring of communications (telephone, Internet, etc.) among many others.

Summary of Information System Privacy Issues

- **Confidentiality of Information.** According to established security policy. Restricting access to information (programs, data, reports, system parameters, etc.) to just those who are entitled to have access — "Need to

know".

- **Inference and Aggregation.** The ability to make inferences from certain information, and the ability to gather together multiple sources of information from which further inferences can be made.

- **Integrity of Information and Systems.** Preventing information (data, programs, systems, network connection configuration information, etc.) from being altered (accidentally or intentionally) in an undesirable manner.

- **Correctness of Information.** Correctness implies that information is input correctly, that it is recorded correctly, and that it persists correctly throughout its lifetime. This is a particular problem in databases of personal information where there are substantive errors in information that can cause serious consequences for the individuals involved. Such errors can occur due to the many varied sources of input data which themselves have varying degrees of accuracy, and any errors can persist indefinitely and spread into other databases and systems.

- **Accountability.** Accountability takes many forms. Ideally, it should be possible to determine who has done what and with what effects within the purview of computer systems and networks. However, audit trails and other accountability measures have serious privacy consequences, which must also be considered.

Privacy-enhancing Technologies and Their Limitations

Computer System and Network Security

To some extent, better system and network security can provide improved privacy protection. However, it must be recognized that many of the privacy violations occur outside of the direct purview of computer systems. That is, privacy is an extrinsic problem as well as an intrinsic problem. Nevertheless, authentication, authorization through explicit access controls, accountability, cryptography, and other technological approaches can help considerably.

Authentication of User and System Entities

- Fixed reusable passwords represent an extremely weak means of authenticating that users are precisely the persons they purport to be. In weak system environments, they tend to be transmitted in the clear when presented to a system, stored unencrypted in memory, written on pieces of paper attached to computers or keyboards, or otherwise compromisible. Passwords associated with individual files are a particularly bad idea. Requirements that persons use hard to remember or frequently changed passwords, while theoretically superior, run the increased risk of persons writing down their passwords and leaving them in easily accessed areas where they may be found and exploited by unauthorized persons.

- One-time never-reusable passwords are next in complexity. The simplest and lowest-tech scheme is the S-Key approach, where a list of once-usable pass phrases is carried by an individual desiring to access a system remotely; the list is generated by a pseudo-random generator in reverse order so that compromise of one pass phrase cannot result in the derivation of the next pass phrase.

- Cryptographic techniques are next in complexity for authentication, as in the case of one-time tokens that are cryptographically generated.

- Various cryptographic protocols exist for authenticating system entities in network security

- Biometrics have some appeal as possible personal authenticators, although there are many problems. In short, human DNA and physical fingerprints are useful for positive identification, and actually can be very valuable in eliminating false identifications; Iris scans are fairly accurate for certain iris attributes, but not always easy to administer and may tend to drift over long periods with respect to certain attributes; face recognition and face geometry recognition are much less reliable. (See the section on biometrics below.)

Authorization and Computer Access Controls

- Access controls for internal privacy management. Access control lists, Unix-like group controls, role-based controls, and various other access control mechanisms are commonly used in attempts to implement policies relating to how information can be used, under what circumstances, and by whom. In addition, there are architectural approaches devoted to capability-based systems (whereby possession of a nonforgeable capability confers certain well-defined access privileges) and multilevel secure systems (for example, implementing a policy in which information cannot move downward from Top-secret to Secret to Confidential to Unclassified, or laterally to different compartments at the same security level). The last of these approaches has many benefits in theory, but has proved to be difficult to implement with sufficient assurance that it cannot be compromised.

System and Network Authentication

- There are extensive techniques for assuring many different types of system-level authentication, such as system-to-system, peer-to-peer, end-to-end, and so on. All of these involve elaborate protocols, many of which are known to have flaws. Developing networks and highly distributed systems that are able to enforce elaborate security policies is an extremely difficult problem.

Cryptography for Enhancing Confidentiality

- Encrypting stored information and transmitted information can be very helpful in increasing privacy within computer systems and networks. However, there are risks related to the handling of that information when it is in an unencrypted form, such as during processing. There are also risks associated with the loss of decrypting keys, and demands from governments, etc. for

"escrowed" access to decryption keys, which can massively weaken the security of all associated systems.

Anonymity and Pseudoanonymity

- **Aliases.** Aliases provide multiple identifiers for the same entity.

  However, aliases do not inherently increase privacy — only perhaps the appearance of privacy.

- **Pseudoanonymous identities.** A pseudoanonymous identity is one that cannot directly be traced back to a specific concrete identity. It may be persistent (lasting over a period of time) or nonpersistent (used only once). The creation of a nonpersistent one-time alias may be more difficult to subvert than a persistent one, depending on the implementation. When used in e-mail, pseudonyms allow recipients to respond to the original sender without knowing the real identity of the sender. However, the privacy of such schemes ultimately depends on the integrity of the anonymizing remailers, and their ability to withstand governmental and other efforts to have them reveal the real identities. There are also serious potential problems with provocateurs using aliases to entrap unsuspecting victims.

- **Blind signatures.** Cryptographic techniques exist that permit authorization of an individual without revealing the identity of the individual.

- **Anonymous smart cards.** Cryptographically based smart cards are more popular in Europe than in the United States. Widespread use of anonymous smart cards is found in prepaid phone cards and prepaid public-transit cards. There is a risk that the identity of the bearer may be known through external surveillance at the time the card is acquired or at the time it is used, but otherwise these cards can provide a certain measure of anonymity. The soundness of the cryptography varies from one card system to another. Furthermore, recent advances in breaking the card cryptography externally imply that there are serious risks relating to misuse of cards and forgery of new cards. In particular, differential power analysis, fault injection, and various other techniques have been demonstrated to be effective in extracting secret cryptographic keys from smart cards.

- **Digital cash.** Various efforts have been made (such as DigiCash and CyberCash) to provide an electronic equivalent of cash, with no traceability. These efforts have not yet been very successful.

Monitoring, Anomaly and Misuse Detection, and Response

- All of the above techniques attempt to prevent unauthorized activities. One other approach is related to privacy enhancement, although it is a detection mechanism rather than a preventative mechanism. Nevertheless, early detection can sometimes be used to prevent further misuse. An extensive collection of systems exists for detecting misuse by insiders and outsiders, detecting intentional and unintentional misuse, detecting system malfunctions, and deviations from expected normal behavior — irrespective of its cause. These detection techniques are particularly relevant to identifying privacy violations (as they are occurring, shortly afterwards, or in retrospective subsequent analysis) and facilitating remedial action.

ID Card Systems

In discussions of identification systems a great deal of attention is often directed toward the specific technologies employed in ID card systems. Often this focus is misplaced since it tends to deemphasize the fact that the range of possibilities for problems, errors, and other undesirable attributes of these systems are often intrinsic to the data being collected itself not to the card system technology.

That having been said, it is still worthwhile to note that none of the highly-touted card systems are foolproof even within the context of their basic security. We are all familiar with common magnetic-stripe card systems where a variety of data is encoded on a magnetic strip typically on the back of a plastic card. It is well known that this technology is subject to a vast range of abuses since the strip (or "stripe") is typically readable and rewritable with easily acquired equipment. The vulnerabilities of this technology have been exploited for years by identity thieves, credit card scammers, and a range of other criminal elements.

In one popular approach, customers who are making purchases unknowingly have the information from their card stripes copied by crooked sales personnel. The perpetrator uses a small device called a "skimmer" to surreptitiously copy the card data when the customer is otherwise occupied. The entire operation can be accomplished in a second or two. Since the magnetic stripe on these cards carries all of the crucial data required to commit frauds, the criminal can then use the collected information not only for orders where the buyer does not need to be physically present, such as mailed, telephone, or Internet orders, but also to generate new physical credit cards that have the ability to be used for fraudulent purposes in stores and the like. Vast sums of money are lost every year through abuse of this card technology. Estimates vary widely, but are approaching billions of dollars, and sizable fractions of a percent of the overall gross.

In recent years a great deal of hype has been generated over the use of so-called "smart cards". These cards, which superficially appear similar to conventional plastic credit or banking cards, include integrated circuitry and usually small amounts of memory which enable the card to operate in a much more sophisticated and supposedly secure manner. While it is true that the information on these cards can not be accessed or manipulated as trivially as in the case of conventional magnetic stripe cards, it has become increasingly clear that the technology used in smart cards is still subject to penetration in many cases using techniques of varying levels of sophistication. (See the illustrative risks section below for examples of smart card vulnerabilities and their exploitation.)

More important than the issue of the technology itself related to these cards, is again the fundamental concern that no system that attempts to collect large amounts of sensitive data on individuals can be made one-hundred percent safe and secure from abuse regardless of the implementing technology. The information in the databases associated with these cards always remains subject to error, falsification, manipulation, and other systemic problems. No card technology can solve this basic dilemma.

It is therefore wise to avoid being oversold by the promises and promotions of the vendors of these systems. In particular, it is critical that the opportunities for error and misuse in these systems be fully understood and evaluated before it is considered acceptable to implement any of these systems, regardless of the technology being promoted at the current time or in the future.

Other Surveillance and Tracking — Photos, Copies, Merchandise

The ways in which ostensibly laudable surveillance can impinge on individual liberties is sometimes very surprising. Most people do not know for example that in the U.S. most photofinishing facilities (places where people go to get their photographic film developed) actively inspect the resulting prints in an attempt to locate illicit images — particularly child pornography. While preventing the spread of child pornography seems like a completely appropriate goal on its face, the real world implementation of these systems has resulted in a range of unfair and embarrassing incidents where completely innocent photographs have resulted in parents being accosted, held, and in some cases even arrested over photos seen by film developing personnel.

These have included images such as very young children without clothing in completely innocent settings such as bathtubs or other home environments and a range of similar locales. The irony of this situation is that in this day and age it is extremely unlikely that genuine child pornographers would take their film to be developed by commercial establishments. It is safe to assume that digital photography, which has no film processing risk, has completely taken over much of the pornographic sphere, particularly child pornography.

Similarly, it is likely that few persons are aware that hidden tracking systems have become common in digital color copiers which can be used to track images back to the machine that generated the original copy (it is likely that this same technology is finding its way into digital printers as well at this time). The ostensible rationale for these systems,

which generally use steganographic techniques to hide a serial number or other identifying information in a manner that is invisible to persons without special technology to decode them, it is to help fight counterfeiting of national currencies on these machines. However, it is obvious that such identification systems could be used in other contexts as well, including civil court cases and a range of other environments since there are few legal restrictions on the use of such identification data.

Again and again we see that the lack of laws to carefully delineate the purposes to which collected data can be put create zones of privacy vulnerability which far exceed the original purposes under which the systems were sold to governments and officials.

Another technology which is likely to see large-scale deployment over the next few years is "RF Tags" — tiny chips which can be embedded in nearly any product or material — which can then be interrogated via radio- frequency systems without the knowledge of the owner or user. These systems are sold as inventory tracking and control aids, but could be subject to abuse in many other situations since they would allow for detailed tracking of the location of these products for an unspecified time into the future after they have been sold. Though the technology only works over a relatively short range at this time, the lack of a legal basis to control the collection, use, and dissemination of this data should be of great concern even at this early stage.

Implantable ID Chips, etc.

A great deal of public attention has been generated around the concept of implantable ID chips. These devices (like the ones promoted by Applied Digital Solutions, Inc. as "VeriChip" and "Digital Angel") are still in their infancy but carry a wide potential for their abuse. Developments in this field suggest that they could represent a tremendous civil liberties risk in the near future, and may well represent a significant risk among certain populations immediately.

While the promoters of these systems like to talk about the ability to implant a device in a person which could be used to locate them in an emergency (children and the elderly are usually mentioned as benign targets in this respect) it is not possible with existing technology to implant a device with such capabilities that would be small enough to be acceptable in most circumstances.

Such a device would require communications capabilities such as an integrated cellular telephone system, GPS facilities, antenna, and power supply, and would likely be the size of an implanted pacemaker — not something that could be simply injected into the skin. Technological developments will no doubt reduce the size of these components considerably but for the immediate future the capabilities of these devices will remain more limited to "simple" identification applications — which are themselves significantly likely to be abused.

Currently available ID chips for humans are essentially the same devices which have been used with household pets for a number of years. These are small encapsulated chips which can be easily injected into the skin on what is considered to be a permanent basis (that is, they cannot typically be removed without surgery). These devices usually contain a unique serial number which can be interrogated over a relatively short range of some feet without requiring an internal power source. The serial number of the chips are then used to interrogate external databases which would include the data of interest concerning individuals. Medical records are frequently mentioned as a positive example for this sort of application, even though the Food and Drug Administration's initial agreement not to regulate these devices was based on their not being used for medical purposes.

It is however easy to visualize how even this relatively crude technology could be highly privacy-invasive if its use were mandated on a non- voluntary basis. Populations with little control over their own rights in this regard could include children, current or past criminal offenders (regardless of the severity of their crimes), even HIV and AIDS victims. In a society where knee-jerk reactions to perceived security and health threats is common, it is not inconceivable that laws mandating the injection of identification chips into such populations would be possible. It would then be but a relatively short leap to widespread mandated use of such devices.

Since the current implanted devices cannot be turned on or off, they would be subject to interrogation at any time, by anyone with the appropriate equipment, potentially without the knowledge of the person being scanned.

Basic human rights should include not being subject to identification in situations where it is not reasonably required. These sorts of technologies, despite the apparent good intentions of their promoters in some cases, carry with them Orwellian possibilities for misuse and abuse of many kinds.

Privacy Risks in Entertainment Technologies

A little noticed but potentially quite significant area of privacy concerns relates to the rapid deployment of technologically sophisticated entertainment systems, especially related to television broadcasting.

Most consumers are unaware of the degree to which their personal viewing activities may be subject to recording, tracking, analysis, and even commercial distribution use by broadcasters and related firms. The opportunities for this sort of data collection are in a number of areas.

The new generations of set-top cable television boxes frequently include the capability for feeding a variety of usage-related data back to the cable operator. Such data can include a wide range of information relating to what channels are being viewed and when they are being viewed. This sort of data can provide a relatively detailed glimpse into the personal interests of the viewer. Most viewers would be surprised to learn that in the absence of specific privacy policies to the contrary such collected personal information could be subject to widespread commercial exploitation.

A similar situation exists in relation to satellite television receivers which use the telephone line for feeding information back to the system operators. While most customers may assume that the telephone line connection is only used to process special purchases such as pay-per-view events and the like, the same facility can also be used to capture and relay a wide variety of other detailed customer usage data.

In the case of the U.S. marketplace, both of the major satellite TV providers for consumers use technology that includes the telephone line connection. While in some cases the systems (EchoStar's "Dish" network and DirecTV) can be operated for periods of time with the telephone line disconnected, it is impractical to do this for long periods if any advanced capabilities or pay-per-view purchases are contemplated. And few customers would have reason to be concerned about the connection in the first place if they did not realize that privacy-related personal information could be passed over that mechanism.

Perhaps the most elaborate example of this issue relates to the TiVo PVR (Personal Video Recorder) system. These units (and their competitors such as SONICBlue's ReplayTV and EchoStar's DishPlayer) record television programming on an automated basis via computer hard disk drives.

A primary facet of these systems is their use of downloaded schedule information which allows for automated scheduling of program recordings and sophisticated search capabilities. In the case of TiVo, units exist that can record either from over the air and cable broadcasts in one instance, or directly from digital satellite TV transmissions, via integrated receivers, as another product. EchoStar's DishPlayer system has similar integrated satellite TV receiver capabilities internal to its PVR system.

With both types of TiVo units, the amount of data that the units are capable of collecting regarding users' interactions is extremely comprehensive. In fact the unit can literally record and log every action that a user makes including every press on the remote control, every program watched, how long programs are maintained and how often they are viewed, and virtually every other aspect of users' viewing and operational habits. Since the system also includes the capability of automatically watching for particular programs based on titles, actors, keywords, and other parameters, it can collect a great deal of data regarding the interests of viewers.

Both TiVo and DirecTV (DirecTV now operates the integrated DirecTV/TiVo system under its own name) have been sensitive to the issues related to the possibilities of abuse of this data. Detailed privacy policies are available to customers, and significant changes in those policies are transmitted to the boxes and at least in the past, have been presented to users before they can proceed with regular use of the devices.

Users have the ability to opt-out of data collection either partially or fully, according to these policies. Nonetheless, in practice, it can be difficult for viewers to actually avail themselves of these opt-outs and be sure that the opt-outs are actually being honored. Customer service representatives have shown confusion when customers request to exercise their opt-out privileges, sometimes having to speak to supervisors and apparently go through manual processes to set up opt-out status. Nor is there any mechanism for the average viewer to autonomously check the status of their opt-out choice and be sure that it is being honored.

Fundamentally, the opt-out remains a matter of faith since the boxes could still be transmitting data and the viewer would have no way to know that their opt-out might not have been effective.

This example is illustrative of a broader problem in the privacy arena, namely that even when there are good intentions relating to privacy policies (though we consider opt-in to always be preferable to opt-out) the real world implementation of these systems can make it difficult for customers to actually avail themselves of these options or verify that they are in place. In this respect, the situation is very similar to that which we discuss relating to privacy policies of financial institutions and credit card companies, where the opt-out provisions that are available may be difficult for users to exercise and verify.

It should be noted that it is likely that this trend toward collection of user data from entertainment related devices and systems will continue to accelerate both in the near and long-term. This will be driven both by commercial concerns as program producers, broadcasters, and manufacturers

attempt to devise new models for income streams (in some cases based on targeted advertising or other demographically linked marketing schemes) but also because of the demands from program suppliers who are concerned about piracy and what they view as misuse of their programming material such as television programs and movies.

The digital rights management (DRM) systems which are being implemented widely to try to control viewer use of programming material and keep viewers on very short leashes would appear to be increasingly and integrally involved with the collection of viewer usage data and tracking of that data in real-time, in the longer-term, and even retrospectively.

This entire area of entertainment technology privacy may be one of the most pervasive affecting ordinary consumers in the course of their day-to-day lives. If suitable and reasonable laws and other regulations are not established beforehand to control the manner in which customers are notified that such data collection will take place, and to enact suitable restrictions on the ways in which that data may be used and disseminated, it could become a highly abusive and potentially coercive force to the detriment of basic privacy rights.

Biometrics

One of the key buzzwords in the identification and privacy areas these days is “biometrics”. Biometrics refers broadly to the use of physical characteristics to aid in the identification of an individual. Examples of this include fingerprints, iris or retina scans, and recently parameters such as DNA — they show physical characteristics and a range of other physical attributes.

Unfortunately, there is a great deal of misinformation, hype, and misunderstandings regarding the usefulness of biometrics data in these sorts of applications. For example, a great deal is being made these days concerning the use of biometrics data with identification smart cards. The assumed principal is that a person presenting such a card would need to also provide a biometrics measurement of some sort to verify (or at least ostensibly verify) that they are actually the person associated with that identity card or other instrument.

A fundamental problem relating to the manner in which biometrics are promoted to government agencies and other organizations, is that they fail to recognize that a biometrically matched identification says absolutely nothing about the accuracy of the data associated with the identification card itself, regardless of whether that data is carried on the card or as is more commonly the case used to index data in external databases.

Knowing that the biometric identification for a person matches (or seems to match) an identification card provides absolutely no assurance that the referenced data including critical aspects of that person’s identification is actually accurate and not subject to either accidental or purposeful error or other manipulations.

In the case of the September 11 hijackers, it is likely that most of them would have been able to obtain perfectly legitimate biometrically-linked identification cards, since most of them were in the U.S. seemingly legitimately (although in some cases with false identities). So even in the presence of a fully developed biometrically-enhanced identity card system, the fact that they matched the identity associated with their cards would not have provided any useful information that would have prevented their activities, even assuming that all of the information associated with their records was entirely accurate.

To make matters even worse, it is not at all clear that biometric technologies provide anywhere near the level of accuracy or assurance that their vendors and promoters would have us believe. In fact, there is considerable evidence that the error rates on these systems are so high as to render their use highly questionable in many critical applications.

In the case of fingerprint identification systems, it has been demonstrated that trivial techniques, including the use of gummy imprints to create false fingerprints, could easily foil various commercial fingerprint identification systems. (A report of Tsutomu Matsumoto's results is given in RISKS, vol 22 issue 8, and detailed in Bruce Schneier's CRYPTO-GRAM,

http://www.counterpane.com/crypto-gram-0205.html#5, spoofing all of the targeted machines, 80% or more of the time.)

Face recognition systems, which have been highly touted as of late as anti-crime and anti-terrorism tools, appear to have abysmal performance in real world situations, with both type 1 and type 2 errors (missed identification and false identification) being major problems. Even under controlled conditions where high quality images were used as templates for testing, a situation that would not exist in the real world, error rates on these systems have proven to be unreasonably high. In fact, there is little if any evidence of any actual arrests resulting from the deployment of these systems in production environments. However, it does appear that the level of false identifications that result can drain the resources of security personnel and actually decrease security.

Other technologies are under development that also play into this arena. These include rapid, automated DNA profiling, experiments with identification of persons from their body odor, and even more esoteric and in some cases somewhat humorous-sounding ideas.

While biometric systems can provide some level of additional security when attempting to verify that the particular person presenting an access card is the person who should have that card, the real world performance of biometric systems in scanning large numbers of people to try point out particular "bad guys" is very poor and apparently impractical at this time.

And as mentioned above, even when a biometric identification helps to assure that a card holder is the "correct" person, it still must be emphasized that it provides absolutely no assurance that information associated with that person, for example whether or not they might be a terrorist, is accurate in any way.

Advances in this technology area are coming at a rapid pace. It is likely that the error rates on at least some of these systems will fall significantly as time progresses. This suggests that concerns about the broader privacy issues associated with the abuse of these technologies for large-scale profiling of individuals and populations will require a great deal of ongoing study, discussion, and concern.

Total Information Awareness (TIA)

Another area of ongoing concern is the manner in which government agencies and/or other organizations could abuse database information which has been collected ostensibly for a limited set of purposes. The issue of "data mining" will do nothing but becoming increasingly critical as time goes on. Once information is collected, regardless of the purpose for which it was collected, it is subject to abuse if it is not rapidly purged.

In the U.S. recently, a great deal of alarm has been expressed regarding the Total Information Awareness (TIA) project of the Defense Department's DARPA agency. This research project was designed to develop the technology to implement and deploy enormous database systems that could cross reference vast quantities of public, private, and government data to create massive dossiers on virtually any individual within its purview. This would include information from intelligence agencies, commercial sources such as banks, credit card companies, and other companies that collect information on individuals' purchases, movements, and other behaviors. Already, vast amounts of information of this sort is collected by commercial firms, with few controls on its use, resale, exploitation, or other activities regarding the data. The specter of this sort of information — which has already been raising red flags among persons concerned with privacy issues — being combined in the manner suggested by TIA has triggered alarm bells all the way to the U.S. congressional level.

In fact, the U.S. Senate recently voted to at least temporarily block or restrict funding of TIA until more information was made available or specific national security issues were identified. Additionally, moves to restrict TIA operations to non-U.S. operations have also been part of Senate activities. It appears possible that the U.S. House of Representatives may take similar actions.

It is important to realize however, that it is highly probable that TIA will continue in one form or another anyway. National security exceptions, and other loopholes, could well provide the avenue for continued development and deployment. Also, developments in the commercial sector among the private and public firms who already engage in vast amounts of information gathering, data mining, and databasing, may well results in systems similar to that envisioned by TIA even if TIA ceased to exist completely. Again, the absence of laws preventing the abuse of data in these manners is critical to the situation and is an area where the U.S. is particularly at risk of major privacy-related problems.

Encryption

In the wake of September 11, there has been renewed discussion of the issues relating to restrictions on encryption technologies. This is an issue that continues to raise its head at intervals. Either an outright ban on the ability of individuals or nongovernmental organizations to use powerful encryption systems, or so-called "key-escrow" systems where the decoding key would be available to the government on demand, are recurring proposals.

There have also been calls to make use of encryption (exactly how this would be defined is not clear) during the commission of a crime a factor to increase prison sentences upon conviction.

The premise behind these arguments is the assumption that criminals, terrorists, and other undesirable elements could use encryption technologies to obscure their communications and further their evil aims. In practice, up to this time, it appears that the use of encryption by such persons or groups is minimal and unsophisticated. Most or all of the terrorist communications related to September 11 apparently were in the clear — unencrypted — and in some cases were even intercepted by intelligence agencies, but not translated, interpreted, or acted upon by authorities in a timely manner.

But powerful encryption systems have enormous roles to play in the protection of individuals' rights and of critical infrastructures. Persons living in countries with oppressive governments have found encryption crucial to their own communications. The importance of encryption to financial institutions — particularly as Internet use has become such a major part of these systems — is obvious, especially given the range of hacking problems that exist.

Any system which attempts to limit the capability of encryption or to force the availability of keys to authorities upon demand, risks undermining the usefulness of the entire technology. Weaknesses will be exploited one way or another, and the mere existence of escrowed keys creates an enormous target for hackers and a gigantic opportunity for abuse by current or future governments. It is always important to remember that even if you have complete and total faith in the persons running your current government, you may not feel the same way about all government authorities in the future.

Fundamentally though, the entire argument for encryption control is largely academic. The techniques and methods for performing powerful encryption are well-known and there is no way to get that knowledge out of the hands of the public. Simple personal computers of the sort found in almost every home in many countries are more than capable of performing high-grade encryption that could not to be broken in a practical sense unless those systems have been rigged beforehand to pass critical information onward to authorities. In fact, this issue of whether or not the hardware and software that people have on computers in their homes and businesses can necessarily be trusted is a major issue unto itself.

Even if all encryption were outlawed there'd be nothing to stop the persons whose activities you were most concerned about from continuing to use it. Only law-abiding citizens would likely be undermined by prohibitions on encryption. It is not even possible to know with certainty when encryption is being employed. Techniques such as steganography can hide data innocuously within other files including audio, video, still images, and others. Properly implemented, such systems are essentially undetectable. (See the following books: Peter Wayner, "Disappearing Cryptography: Being and Nothingness on the Net", Academic Press, Chestnut Hill, Massachusetts, 1996; Peter Wayner, "Translucent Databases", Flyzone Press, Baltimore, Maryland, 2002; Stefan Katzenbeisser and Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House/Horizon, 2000.)

One way or another encryption is with us to stay, and its use is crucial not only to personal privacy issues, but to critical infrastructural issues as well.

Internet Privacy Issues

When considering privacy issues relating to the Internet, it is important to remember that at the present time the vast majority of traffic on the Internet, that is generated or received by ordinary users, is not encrypted in any manner. Data "in the clear" of this sort is therefore vulnerable to interceptions (either legitimately by government officials or illegitimately by anyone) who has access to any of the many computers, switches, routers, and other equipment, that are in place between the sender and receiver of the data.

While the next generation Internet backbone system (IPv6) will have encryption capabilities designed-in at its basic level, the adoption of its new protocols has been very slow and the longer-term future for IPv6 is not entirely clear at this time. IPv6 is still not a complete solution, as it provides only rudimentary measures for authentication and encryption for confidentiality. Preventing denials of service on the network infrastructure remains a huge problem.

While there exist a variety of easily available and even free high-quality encryption packages for the use of ordinary computer users on the Internet, most people don't use them. Many persons feel that their information is simply not valuable enough to be worth the hassle of protecting through encryption. On the other hand, the "hassle-factor" inherent in using many of these encryption systems can be a major issue even for those users who would prefer to keep their data securely encrypted as it travels the Internet.

As the Internet has become very much a utility for transmission of all sorts of important personal information ranging from financial and medical data through a vast range of other applications, the continued use of unencrypted systems for many of these important applications cannot be tolerated.

One of the most obvious areas where encryption provides immediate value is to protect e-mail transmissions. Software called "PGP" ("Pretty Good Privacy") is available for free or for a nominal charge and can be used for this purpose. (See http://www.pgp.com.) However, even it tends to be unwieldy enough to use that many potential users don't bother with it most of the time.

A perhaps more promising development for e-mail security on the Internet is the gradual spread of the STARTTLS (Transport Level Security) system which can be embedded within standard mail transfer agents such as sendmail and various others. The STARTTLS system provides the opportunity for opportunistic encryption of e-mail, automatically encrypting the e-mail traffic between suitably capable machines without any actions being required on the part of the persons who are actually sending or receiving the e-mail. While the STARTTLS system is still vulnerable to "man in the middle" attacks unless used with prearranged digital certificates, it still provides a significantly greater degree of security and privacy than e-mail that is sent unencrypted in the clear.

Spyware

Another area where Internet users' personal activities and information may be surreptitiously funneled to third parties relates to the type of software known colloquially as "spyware". Spyware can be broadly considered to be any software which a user might install on their computer unknowingly (typically as part of a desired, downloaded software package) that surreptitiously collects, tracks, or otherwise obtains information about the user's computer and/or activities and sends them over the Internet to third parties.

Examples of some of the software systems that meet this classification include hidden keystroke monitors such as the CIA's Shadow program that allows its supervisors to remotely monitor their employees' computer usage. The FBI's Carnivore system (now called "DCS-1000") has considerable ability to monitor Internet communications (see below). Commercial intrusion detection systems also provide considerable information in their audit trails that can easily be misused. A range of commercial programs and hacker tools for "secret" remote computer monitoring also exist.

Specific examples of privacy violations resulting from surveillance are noted below in the illustrative risks section.

The presence of spyware embedded within another application is sometimes theoretically revealed within the privacy policies and "terms of use" of the primary software package that the user has downloaded and installed.

However, given that most users do not read these usually long and complicated disclaimers, it is unlikely in the extreme that most users are aware of the extent to which spyware activities may take place on their computers. Making this situation even worse is that it is not always easy to remove spyware from your system, even after uninstalling the primary software package itself.

Remarkably, some forms of spyware by and large appear to be legal in the United States, since they have not been the subject of significant ongoing adjudication. However, as abuses involving spyware continue to come to light, it is expected that this area could well be subject to significant litigation and perhaps, ultimately, necessary regulatory focus.

Telephone and Pager Communications Privacy Issues

The situation regarding the privacy of telephone calls, pager messages, and similar communications activities is confusing and unclear in the U.S. Part of the reason for this is the hodgepodge of conflicting laws which affect these various communications media. In many cases post-September-11 laws such as the Homeland Security Act and USA Patriot Act have further confused this situation by changing or overriding various existing laws at the national and state levels.

Generally speaking, there has traditionally been a fairly high burden for the government to obtain permission to legally listen in on voice communications. This would typically require some form of subpoena, warrant, or other court order, except in exceptional circumstances (e.g., very limited national security situations). These burdens have been very significantly reduced by post-September-11 legislation.

This environment is also murky (and has been for a long time) relating to private party recording of telephone conversations. This is the kind of situation that applies for example if one party to a telephone call wants to record the conversation in which they are taking part. Individual states have different rules concerning this sort of activity.

Most states are what is called one-party states, where as long as one party to the call knows that it is being recorded the other party or parties do not have to be notified. Obviously, this normally means that the person who wants to make the recording can do so without notifying the person(s) they are speaking to in those states. Some states are what is called two-party states. In these states, it is required that both parties to a call be notified if one person involved in the call wants to make a recording. This obviously is a much more stringent requirement, and in the case of calls involving multiple parties, applies to all parties on the call.

This situation gets extremely complicated if a call is interstate in nature and leaves the confines of a single state's rules. The federal standard for this kind of communication recording by private parties is the one-party rule. However, for calls that are totally within a single state, generally that state's rules take precedence. If a call is made from or to a state that has a different set of rules than the other state (e.g. from a one-party state to a two-party state or vice versa) it is difficult to know what rules will ultimately apply.

Courts have ruled in different and often conflicting ways regarding this kind of situation. An example of this is the notorious case of Linda Tripp who was recording her conversations with Monica Lewinsky on an interstate basis (regarding Lewinsky's affair with then President Clinton). While Tripp was ultimately not held to account for this activity, it appears that had it not been for earlier immunity agreements she might well have been prosecuted for her interstate recordings. However, there is no way to know for a given call how courts may rule on this issue.

In order to deal with this confusing situation, many organizations who generally record (or monitor, for which the same rules generally apply) their calls in the United States, will routinely begin the call with a automatic announcement that the call may be monitored or recorded. This will typically meet the requirements of the law in any state since since it is assumed that if the caller continues the call in that situation they have effectively given their permission for the recording or monitoring.

It should be noted that most of these rules apply equally to landline and wireless/cellular telephones, and in particular, recent changes in national laws have made it more practical and easier for law enforcement to track users in mobile cellular environments. Voicemail messages are subject to yet another set of confusing rules in this regard. Also, in most states, the same rules that apply to recording of telephone conversations tend to be used by courts to deal with situations that arise regarding person to person recordings, that is, physical meetings of people where one party records the conversation without the other party's knowledge.

The rules are also quite confusing regarding numeric and text based technologies such as pagers. Generally, courts have ruled that information related to setting up a communication has a lower burden for the government to obtain that information than does the content of the communication itself. So, for example, the government can more easily obtain records of phone numbers that were dialed (thusly providing information about the location to which a caller was speaking) than they can gain access to the actual contents of a call.

Oddly however, courts have also ruled that the contents of pager messages do not necessarily fall into the same category as the contents of telephone communications. That is, courts have tended to rule that the contents of a pager message can often be obtained with the same low burden that the number dialed for a call can be obtained, even though the contents of a pager message are much more analogous to the contents of a voice communication.

It is not clear how these rules will be interpreted with the advancing changes in numeric and text based technology, for example concerning government requests to obtain the contents of alphanumeric pages as opposed to purely numeric pages, or similarly for the contents of text messages that might be sent to other wireless devices (e.g. cellular/wireless

SMS messages) and other new technologies. This is clearly an area where court actions and litigation are probable to clarify the situation, however in the current environment, it is likely that rulings will give the government increasing powers to obtain this sort of information with increasingly lower burdens being required.

Monitoring and Surveillance

Supermarket Loyalty Cards

The pervasive nature of tracking systems in the commercial sphere is becoming truly awesome in its extent. One of the most frequently seen and increasingly controversial tracking technologies is the so-called supermarket loyalty card. These cards, which are typically barcoded, are used by customers at checkout time to associate their purchases with their previously registered address and other identifying information. The card itself (which may be the size of a credit card and/or a much smaller keychain-sized card) is merely an index to that database. Customers who forget their cards will frequently simply provide their telephone number to associate their purchases on a particular day.

The ostensible purpose for the supermarket loyalty card systems is to provide customers with discounts on their purchases. Indeed, the vast majority of discounted prices in supermarkets issuing these cards (which now includes most major chains) are restricted to customers who are willing to participate in these loyalty card programs. There has been considerable concern that prices have actually been raised in many cases for non-loyalty card participants in order to make the prices appear lower for those who do participate.

While some of the participating supermarkets have specific privacy policies associated with these programs, they are usually drawn in terms that do not strictly control the manner in which the information collected might be used. Even when these policies suggest that information will not be provided to outside entities, it is still possible that the range of uses within the corporate family or in some cases the associated partners permitted by the privacy policies could still be abusive.

As in other industries, the consolidation that has taken place in this market segment means that even when collected information can only be officially used within the corporate family, a large number of varying entities may fall under that permissive umbrella.

The loyalty card systems will typically create a record of every item purchased by the customer and associate it with their database identity. This is accomplished through means of the barcoding systems now ubiquitous on virtually all products. There also indications that some supermarkets may be planning to move toward RF tag systems which will have even greater capabilities. These will be tied to transponders on supermarket shelves for a variety of additional applications.

It can be argued that the abuse potential for supermarket purchases tracking is relatively low — at least in compar-

ison to many other kinds of collected information. However, is always important to remember that loss of privacy is an incremental process. It occurs little by little from varying directions. One day you turn around and you find yourself naked of privacy even though the individual elements of your privacy appeared to be jeopardized only slowly over a long period of time.

Supermarket tracking data has already become the subject of legal actions attempting to ascertain whether specific persons have made particular purchases related to civil actions or criminal cases.

The negative reaction to supermarket loyalty card programs among a vocal minority of customers has resulted in imaginative techniques for foiling the system. There are organized groups who trade their supermarket identity cards on an ongoing basis. Even in the course of normal purchases is not uncommon to find one customer lending their card to another who has forgotten to bring their own to the checkout line. While it can be presumed that such actions have only a minor impact on the overall quality of the data in these databases, it still demonstrates that such data even in this relatively simple case cannot be depended upon to be entirely accurate and free from various kinds of systemic errors.

Cashless Society, More on Tracking

It should be clear to any observers that calls for moves towards "cashless societies" will generally entail major privacy risks due to the intrinsic tracking capabilities of these systems as typically deployed. While it is theoretically possible to design such systems in manners that would allow for anonymous transactions or with rapid expunging of transaction data, there has been little interest on the part of government or other organizations toward development of such privacy-protecting capabilities. In fact, the exact opposite has proven to be the case.

While it is obvious that environments such as electronic signature systems usually require non-anonymous and long-term recordkeeping activity, there are a range of applications where those requirements do not exist from a technical sense yet are still exploited by government.

An example of this is the handling of electronic toll collection systems such as EZPass and FastLane, which allow commuters to automatically pay their tolls without stopping (for tollways, bridges, etc.) via small electronic transponders. It would be completely feasible for municipalities wishing to use automated toll collection systems to support the technical means to bill commuters appropriately without collecting and storing detailed data on persons' movements, or as an alternative to rapidly expunge the data concerning such movements after the current billing cycle.

Unfortunately, it appears that municipalities in general have chosen to maintain such data indefinitely, in the hopes that it might have some future value. Already we're seeing cases of courts and other legal actions where this sort of data is being requested by attorneys, law enforcement, etc. This was inevitable so long as the data exists.

A basic tenet of good privacy policy is that information that is not needed should not be collected in the first place and certainly should not be stored for long periods. The mere existence of the data invites retrospective abuse.

We see this phenomenon repeatedly across the entire spectrum of privacy issues. Automotive control systems designed to operate airbags and other sophisticated vehicle electronics are creating logs which can find their way into court cases and other environments unrelated to their original purpose. While this may be a boon to insurance companies who are investigating accidents, it is yet another nail in the coffin of privacy since few drivers have any idea that this sort of data collection system may exist under the hood of their car. Some municipalities are now considering the installation of radio based systems to report pollution control information on an automated basis from vehicles. As usual, little or no thought is being given to how that sort of collected data could be abused, which would contain location sensitive information.

Web Tracking Abuses — Cookies, Web bugs, etc.

A number of developments on the Internet's World Wide Web have facilitated the increasing spread of tracking. In the U.S., there are few if any laws that directly control this area. Perhaps the most well-known aspect of this problem are the so-called "cookies" that an enormous number of Web sites now use. Cookies are small bits of information that are stored either temporarily or for longer periods on Web users' computers. Ostensibly, cookies provide state control to manage complex web page interactions. While it is true that they can be and are used for this kind of relatively innocuous purpose, and other relatively benign (though somewhat risky) applications such as saving user passwords, cookies are also widely abused for tracking purposes.

In fact, most of the more egregious systems for the surreptitious collection of user data on the World Wide Web, are based on cookie technology, which will frequently allow for the collection of data concerning users' movements from site to site, data which can be funneled to central organizations without the user's knowledge or explicit permission. While there have been some enforcement actions relating to

this area the practice of abusive cookie use continues to be extremely widespread.

Newer Web browsers have introduced more sophisticated means for users to control cookie use, though it appears that relatively few users actually make use of these to any great extent. This is not surprising, since turning off cookies can cause many major sites to not work properly at all for the user. And systems for specifying which sites should or should not be permitted to use cookies may be confusing to average users.

Attempts to codify Web privacy policies and their interaction with cookies on an automated basis, such as the Platform for Privacy Preferences (P3P), are highly controversial. There are concerns that these artificially constructed mechanisms for attempting to enforce complex privacy policies may be misleading to users and result in a range of complicated legal battles and other undesirable effects.

The conflict between P3P-type mechanized privacy rules and the actual privacy policies that have a force of law on Web sites can be highly significant. The actual privacy policies tend to be complex and written in legal language that few users take the time to read and fully understand. Yet it is this form of a privacy policy that would appear to represent the force of law, not necessarily the simplified automated privacy policy presented by P3P or similar systems.

Another aspect of Web privacy violations that is perhaps even more insidious than cookies is the area of "Web bugs". Web bugs, which are also known under other more innocuous terms such as "clear gifs", "invisible gifs", and "beacon gifs" are tiny invisible images transmitted on Web pages. These images, when processed by a user's Web browser, provide information about the viewers' activities back to the site presenting the Web page.

Essentially, whenever a Web page is presented to a user, all images referenced from that page must be retrieved from the appropriate Web server (which may not even necessarily be the same server presenting the other portions of the page). Every retrieval of an image or other information from a Web site will typically leave a detailed log record which can be analyzed either in real-time or retrospectively. Used in conjunction with cookies — or even simply used by themselves — Web bugs provide yet another avenue for tracking user activities. Web bugs are particularly of concern since effective mechanisms to control them are largely nonexistent in most current popular Web browsers relied upon by the vast majority of Internet users. Web bugs use has become extremely common even by reputable organizations who fail to recognize their intrusive nature.

The issue of Web bugs points to the broader privacy concerns regarding Internet e-mail. The rise in use of "HTML" e-mail, that is, e-mail including elaborate capabilities for formatting, fonts, and other elements that go far beyond traditional simple text, intrinsically includes privacy violating elements.

Anytime an HTML e-mail message is opened by the user (when they are connected to the Internet) any images or other retrieved elements included in the e-mail will behave exactly like Web bugs. This kind of facility has become widely used including in some popular commercial e-mail products to track not only who has initially opened and read e-mail and when they have done so, but even the ways in which e-mail is forwarded from person-to-person.

The combination of cookies, Web bugs, and HTML e-mail, has created a veritable witch's brew of privacy risks and violations. Yet these highly negative features are not understood by most users, and are almost completely free of regulatory scrutiny. It is likely that these problems will only become worse with time unless steps are taken immediately to establish some sort of regulatory framework for their control.

Abuses of Web-collected Information

The vast amount of personal information that many Web sites collect from users, either indirectly without their knowledge or directly with their explicit participation, has created vast databases of information which when correlated with other sources of data (such as credit records, banking records, government public record data, etc.) risk the creation of immensely detailed dossiers on virtually every one of us. Since there are few restrictions on the movements of such information between commercial firms or in many cases even to and from government, the information from disparate sources can be correlated by sophisticated database systems to an astounding degree of specificity.

Even when users believe that the information they provide to a Web site will be protected by a particularly stringent privacy policy, they may later learn that their assumption was unfounded. For example, there have been a number of cases where companies in financial difficulties (such as failed dot-coms) have sold or attempted to sell their customer database information to a different firm that had entirely different privacy policies. This has resulted in a great deal of controversy and some enforcement activity by the U.S. Federal Trade Commission (FTC).

Basically, it is unwise for anyone to assume that the information they provide to one entity under a particular set of privacy rules, will forever be either maintained under those rules (which may be subject to change at anytime) or

that the information will even remain soley with that entity.

Lack of specific legal and regulatory frameworks to clearly spell out the circumstances of how such data will be protected and to what extent individuals must be clearly informed ahead of time of the possibly surprising ways in which their data may ultimately travel to other organizations and other uses, have left us in a highly vulnerable situation in terms of these very significant privacy concerns.

Internet Monitoring

In addition to monitoring of Internet and computer activity on the part of government including law enforcement, as embodied in systems such as Carnivore/DCS-1000, programs that can be surreptitiously installed on PCs for government monitoring use, and various keyboard monitoring devices, these same sorts of technologies are now finding use in the private sector.

It is increasingly common for businesses to monitor and track the computer activities of their employees in the workplace and sometimes even on their home computers when linked to business activities. Such monitoring can include tracking of Web sites visited or much more elaborate systems that can monitor virtually every aspect of a person's computer use down to the last keystroke, including program activity, e-mail, and all other aspects. Some of the more controversial aspects of such monitoring come about when employers fail to notify their employees that this monitoring may be taking place.

While there have been attempts in some areas including the state of California to mandate that employers give such notice to their employees before monitoring may occur, such notification is still a rarity and is generally not required by law.

A perhaps even more complex situation arises when private individuals make use of such monitoring technologies to spy on their family members including spouses and children, etc. The reasons for such monitoring can be many and varied but typically revolve around obvious concerns such as children's Web site activities that a parent may view as potentially hazardous or undesirable, concern over spouses' communications with and possible interactions with other possible love interests, and similar sordid activities.

By and large U.S. courts have not established any consistent set of rules or guidelines for determining when such activities within a home are legal or to what extent information collected from such activities can be used or released, leaving vast areas of concern relating to the conflicts between freedom of speech, parental and spousal rights and community property, etc.

Global Positioning System

The rise of small and inexpensive global positioning system (GPS) satellite receivers has introduced yet another facet to privacy concerns. Already there have been incidents of GPS systems being used for surveillance both in the public and private environments. GPS receivers when integrated with wireless technology such as cellular systems, enable the creation of compact tracking devices which can use GPS to accurately pinpoint locations, and the wireless networks to transmit resulting location information to a party who could be anywhere on the planet.

Recently, there have been several highly publicized cases of stalking-related arrests of individuals who have used such devices on others' vehicles in an attempt to track their activities. Again, the exact legal status of the systems is unclear and has not been subject to adequate analysis by U.S. courts to establish reasonable guidelines as to situations in which their use is clearly legitimate or clearly illicit.

Video Surveillance

One of the most obvious developments in recent years has been the radical acceleration of the use of video monitoring systems throughout the world in a wide variety of situations. Cameras and related cameras systems seem to permeate our world from surveillance systems in stores and businesses to cameras in a wide variety of public places. The reasons for the use of such systems range from security to voyeurism, and the users range from private businesses to government officials to private individuals.

Government use of video systems now runs the gamut from traffic observation to automated stoplight violations systems to public camera systems explicitly designed to try prevent or reduce crime in public areas. Cameras seemingly can be placed in virtually any public space with few limitations of any kind. Most citizens appear to be reasonably happy with the appearance of this massive big brotherish surveillance deployment, being convinced by government assessments that it will improve their security.

Lately, increasing numbers of these video systems have been tied to face recognition systems with the claim that they would help the find terrorists or other law violators. There appear to be few limits on the ostensible targets of these face recognition systems with some locali-

ties suggesting that they would be useful to find deadbeat dads who have failed to file child support payments on a timely basis.

Notwithstanding the fact that the real world performance of face recognition systems has proven to be abysmal in terms of actually finding terrorists or other criminals, and the extremely high error rates of these systems, the appearance and acceptance of these systems suggest the lack of understanding by the citizenry of the risks that this sort of surveillance represents. Even if one fully trusts current government officials and authorities not to abuse such systems, there is no way to know how future governments and officials might abuse these infrastructures which once established are very difficult to remove.

A frequently heard refrain from officials when confronted by persons who are concerned about such surveillance systems is that individuals "have no expectation of privacy in public places." This includes apparently simply walking down the street as well as events such as the National Football League's 2002 Superbowl, where face recognition systems have previously been deployed. In reality, this argument is utterly specious. Unless we are willing to take the view that individuals must remain within the confines of their homes at all times, it is clear that intensely personal and detailed dossiers of a person's activities, simply in the course of their day-to-day actions, can be made solely from the cameras and other interconnected surveillance systems placed in public places.

If individuals found themselves being followed by men with clipboards noting down everything they did and everywhere they went in public, it is likely that few persons would tolerate such surveillance. Yet the presence of camera systems in public places is becoming very much an equivalent to that sort of intensely personal surveillance, it simply is less obvious to the targets.

The abuses resulting from the misuse of video surveillance technologies also extend to the private sector. Employers spy on their employees in a variety of situations. It is not always clear when such surveillance is legal from state to state, especially if audio is being recorded or received along with the video or if sensitive locations such as restrooms or clothes changing areas are involved.

Private sector abuse of these technologies also extends to individuals. In this category we find a range of persons who have created effectively an entire industry out of the use of tiny cameras for voyeuristic purposes. Such cameras have been found in restrooms, gyms, even in private homes and apartments planted by landlords. The images from these cameras may be used for the private gratification one person, a group, or frequently may be sold on the Internet or other venues. The term "upskirt" has been coined to refer to the use of these small cameras to look up women's dresses in public places, etc.

Remarkably, even this sort of activity is not clearly illegal throughout the U.S. in a general sense. Some states have moved to introduce laws affecting this area, but there are no national standards as of yet.

The easy availability of this technology has also resulted in disputes between neighbors where one party uses cameras to place under constant surveillance a neighbor for any of a number of purposes. Generally speaking, such activities, though highly upsetting to the target, are often found to be legal so long as the person with the camera is on his own property, public property, or otherwise has not actually invaded the space of the individual being surveyed. As might be expected, this has also become a highly contentious area where further legislative and court action is drastically needed.

Cellular and wireless technologies

The rise of ubiquitous and inexpensive cellular and other wireless networks have introduced yet another complex aspect to privacy issues. Cellular telephones even several years old can often be configured in ways that turn them into ideal audio bugging devices. The simple attachment of a remote microphone (unnecessary in some cases) and setting the phone's modes to not make any of the normal audio activity (beeping) sounds, along with activation of auto-answer modes, can result in a small, "off the shelf" bugging device that can be accessed from anywhere in the world so long as the batteries in the cell phone will last. If an external source of power has been provided such activity can go on indefinitely.

Concerns over such possibilities have resulted, perhaps belatedly, in actions to try to prevent such use of phones within organizations with obvious security concerns regarding such bugging.

Cell phones can also be integrated with inexpensive global positioning system (GPS) equipment to feed location data back to a source who could be virtually anywhere.

More recent generations of wireless phones have taken a quantum leap toward enabling even more possibly intrusive activities in this regard. Newer cellular phones tend to be smaller, more unobtrusive, have much longer battery capacities, and in general make even better bugs than their predecessors. The new availability of still camera devices which can be attached or are even integrated to new generations of wireless phones opens up an entire new

avenue of surveillance and bugging use for these devices.

They enable not only the sending out of audio surreptitiously, but now the sending of still images and probably soon moving images as well. The obvious opportunities for abuse of such systems range from “simple” voyeurism to industrial and anti-government espionage. Already, it has been announced that use of video equipped cell phones will be prohibited in some areas (such as gymnasiums in Hong Kong).

What the rise of this technology shows us, yet again, is that the typical government approach to dealing with privacy issues, which is to approach them on an after the fact basis, is wholly inadequate to the rapid pace of technological change, so much of which has detrimental effects on privacy rights and related concerns.

Anomaly and Misuse Detection, and Response

Research in anomaly detection and misuse detection systems goes back several decades. In the past 5 years or so, commercial systems have become widely deployed. Commercial host-based and network-based systems are common, although problematic in that they tend to have false-positive detection rates that are too high and that put an enormous burden on administrators. Companies such as Counterpane provide a way of outsourcing a company’s analysis. However, because there is a considerable amount of sensitive information in the audit trails and in the resulting analysis, outsourcing tends to expose a company or a government to risks of third-party untrustworthiness.

Illustrative Cases of Identity and Privacy Risks

The archives of the ACM Risks Forum moderated by Peter Neumann contain hundreds of examples of privacy violations and discussions of privacy-related issues. See the following sources for background.

- www.risks.org for the searchable archives of every issue since Volume 1 Number 1, 1 August 1985.
- Peter Neumann's book (Computer-Related Risks, noted in the Bibliography).
- Many of the monthly Inside Risks columns in the *Communications of the ACM*.
- A list of thousands of examples of computer-related risks, including a very large number of cases related to security and privacy problems and privacy violations.

We list here a few of the major privacy-related risks and illustrative examples.

Identity Problems

All sorts of problems are attributable to the use of identifiers, resulting from wrong names, multiple names (aliases), ambiguous names, confused names, forgotten names, impersonations and other unauthenticated identities, and, in some cases, the absence of identifiers altogether. Mere knowledge of a name or identifier can lead to harmful acts against an individual. All of these risks arise in computer-related systems and in life situations, often in combination with one another.

- **Misuse of fingerprint system.** Martin Lee Dement spent 2 years in Los Angeles County Jail, because of botched use of the then-new California Automated Latent Print System. Manual check of another suspect's prints finally cleared him.
- **Evidence to the contrary.** Joseph O. Robertson was arrested, extradited, and confined to a state mental facility for 17 months, despite available mug shots and fingerprints that subsequently exonerated him.
- Sheila Jackson was arrested, jailed, and given a computer arrest record with an alias for her married name, because of an NCIC hit on an outstanding warrant for someone named Shirley Jackson.
- Donny Ray Boone spent 41 days in jail in Florida because of a confusion with a similarly named individual (Bone?).
- In Montreal, two people named Steven Reid had the same birthday, with expected consequences. Lt. Gerard Blouin of the Montreal Police stated, "It's up to him to change his name somehow. If he can modify his name, just by adding a middle initial or something, it would help him."
- Two people named Neil Fosters both living in the Boston area had similar appearances. The wrong one was apprehended after a query on the database produced a match on incomplete information, with unfortunate consequences.
- Two people named Shirley Jones had different birthdays, heights (6 inches apart) and weights (70 pounds apart). The wrong one was arrested despite the obvious disparities, while the real suspect was already in jail.

* Anne Marie O'Connor and Ann Marie O'Connor in the New York City area unknowingly shared the same SSN. They also looked similar, and both had birthdays in September. This situation was discovered only when one of them was dunned for back taxes on their combined incomes!

- Two men in New York named James Edward Taylor shared the same birthday, birth state, and SSN. This situation was first detected in 1965, but had still not been corrected when reported in 1973.
- New York's Blue Cross health-care computer system was unable to distinguish two hospital patients with same gender and birth date, and created awful billing and payment problems as a result of twins and triplets being treated by the same doctor on the same date. Considerable annoyance resulted for patients, parents, and doctors.
- A masquerader obtained a bogus "duplicate" driver's license for Teresa Stover from the Motor Vehicle office in Bailey's Crossroads, Virginia, which was then parlayed into $30,000 in credit-card charges. The same DMV branch was discovered to have issued thousands

of bogus licenses, allegedly for only a nominal bribe.

- Felonies for stealing, selling, or otherwise misusing SSNs are on the rise in the United States. In 1991, there were already 550 felonies recorded. Someone discovered that 12 people were fraudulently using her SSN, another person found that someone using her SSN had obtained 16 credit cards in her name and had charged $10,000, and a third discovered that her unemployment benefits had already been collected by five other people!

Many different types of problems can arise from supposedly unique identifiers (SUIDs), such as license plates and SSNs, not so much because of the existence of those identifiers, but rather because of the numerous possibilities for their accidental or intentional misuse. Examples include an agency improperly assigning an identifier, a masquerader fraudulently obtaining one, or someone making queries that cross-link disparate databases or otherwise gaining access to information from which information and inferences can be drawn.

Imposition of stricter administrative requirements and judicial penalties might help to ensure the quality of computer-database entries, with respect to both correctness and timeliness of information. False identifications could be reduced if positive matches are never based on partial information without further confirmation. Similarly, negative identifications could be achieved in cases where the wrong person has been apprehended, simply by insisting on a confirmation based on complete information. For example, more thorough forms of low-ambiguity authentication such as biometrics (fingerprints and other fairly unique physical characteristics) can also reduce the probability of false identification, and should be required when lives are at stake.

There are serious risks associated with relying on supposedly unique identifiers, some of which are noted here. Whereas SSNs and other SUIDs are potentially wonderful for avoiding false identification (but break down in cases of multiply used or bogus SUIDs), they are useless for authentication. Unfortunately, these two fundamentally different functions are too often confused. Finally, more stringent policies need to be established and uniformly enforced regarding the use of databases and identifiers — especially across different systems. (See Chris Hibbert's discussion of SSNs, "What to Do When They Ask for Your Social-Security Number. Social-Security Number FAQ (Frequently Asked Questions)." (http://cpsr.org/cpsr/privacy/ssn/ssn.faq.html).

Identity Theft

Many people believe they have nothing to hide because they live an honest life. The ubiquitous use of information about a person's identities and personal lives, combined with the ease of accessing that information, make possible not only inference and aggregation of that information, but also masquerading as that person. This has resulted in an ever-increasing business model of rings of thieves acquiring personal information and then proceeding to strip the victims of their well-being. Identity theft is now becoming an industry in its own right, with massive acquisition of personal data sufficient to do serious damage on a large scale.

Numerous illustrative cases are included at http://www.csl.sri.com/neumann/illustrative.html if you click on "Identity Theft".

- After Terry Dean Rogan lost his wallet (which contained his driver's license and credit cards), someone impersonating Rogan committed two murders and two robberies, which resulted in a warrant being placed in the National Crime Information Center (NCIC) database. Rogan was arrested five times in 14 months, despite trying to get the NCIC records corrected after he discovered the problem on his first arrest. He eventually sued and won $55,000 from the Los Angeles police.

- Richard Sklar was apprehended three times on computer checks because of the activities of a masquerader.

- Clinton Rumrill III had credit-card and traffic problems resulting in civil and criminal charges against him. A childhood "friend" was impersonating him by using his name and social-security number. Police are aware of the problem, but their computers believe that the two are actually the same person. Rumrill was told that the easiest solution would be for him to change his name and SSN.

- San Francisco attorney Charles Sentman Crompton II was plagued by an impostor who had used his name, address, and SSN to establish charge accounts, to rent an apartment, and to get a driver's license. This activity resulted in $3000 in bills. The impostor was arrested numerous times, including for car theft, and each time gave Crompton's identity. Crompton was given the phony driver's license when the impostor dropped it fleeing from a suspicious clerk. He forwarded a copy of it to the DMV, explaining the situation, and asked

for a new license — with a different identifying number. Unfortunately, the DMV mailed the new license to the impostor, further compounding the problem.

- In California, the DMV creates many opportunities for identity theft: in 1999, 100,000 of 900,000 duplicate license requests were fraudulent! (RISKS 21 07); identity theft cases often involve California driver's licenses as primary IDs (RISKS 21 29-32,36)

- California birth records were acquired by RootsWeb.com, placed on the Internet; increasing risks of identity theft? Opt-out only (RISKS 21 80); as a result of heavy responses, the entire databases for California and Texas were removed. (RISKS 21 81)

- Abraham Abdallah was arrested while picking up equipment for making bogus credit cards; he had data-mined SSNs, addresses, birthdates, etc., for 217 of the people on Forbes Magazine's list of the richest 400 in the U.S., also had 400 stolen credit-card numbers; caught trying to make $10M transfer. (RISKS 21 29)

In the past few years, identity theft has increasingly become a serious problem. As we write this, there have been two particularly serious cases just in the past few months, most spectacularly a massive identity theft ring that was broken up, after having victimized 30,000 people, and a second case in which personal information was compromised relating to 500,000 military-related people.

In the first of these cases, billed as probably the largest yet in the U.S., at least 30,000 people have been victimized as a result of an employee of a Long Island NY software company using a Ford Motor Credit Company code to access Experian. He obtained credit histories on people at the request of an identity theft ring operating in Brooklyn and the Bronx, to whom he sold that information for $60 per record. Together with information the ring had already obtained, this enabled them to clean out the victims' bank accounts, make bogus loans, max out existing and newly obtained credit cards, etc. This operation had apparently been going on for three years, until — in response to numerous complaints — the FBI was able to arrest three people, who appeared in court in Manhattan. See the Risks Forum, vol 22 number 40 (http://catless.ncl.ac.uk/Risks/22.40.html).

In the second case, SSNs and other personal information for 500,000 military personnel and family members were stolen from hard-drives belonging to Phoenix-based TriWest Healthcare Alliance on 14 Dec 2002. A $100K reward was offered. Coincidentally, DoD is in the process of computerizing medical records of all military personnel. See the Risks Forum, volume 22 number 46 (http://catless.ncl.ac.uk/Risks/22.46.html).

Other identity thefts in the past few months include these (at Feb 2003):

- Alleged ID thief accused of identity theft on 12 Boston lawyers, using birth certificates and credit reports, evaded authorities for a year; previously convicted of fraud (RISKS 22 20)

- Online job listing leads to ID theft scam via bogus `background check' (RISKS 22 35)

- 4MyEmergency.com gathers personal info in case of disaster, ripe for misuse (RISKS 22 26)

- Busboy pleads guilty to ID theft (RISKS 22 28 and 29)

- Potential ID theft risk in X-Box gamezone (RISKS 22 39)

- Identity thieves create change-ebay.com with a stolen credit card, scam obtains eBay user names and passwords (RISKS 22 40,43)

- H&R Block employees suspected of identity theft against 27 customers (RISKS 22 46)

- 19 people charged with identity theft in filing thousands of bogus tax returns netting $7 million in refunds (RISKS 22 54)

Surveillance

- The FBI's Carnivore system is capable of extensive monitoring of Internet traffic. However, the FBI discovered that an improperly configured system can easily violate the supposedly imposed limits against over-collecting information. (RISKS 21 08-09, 22 11)

- Unencrypted Secret Service pagers were intercepted, despite demonstrations of the risks thereof 3 years before at Hackers on Planet Earth (RISKS 19 39 and 19 40)

- The State of Connecticut routinely recorded every out-

going phone call that newly arrested persons are permitted to make, for several years until this practice was detected.

• Risks of concentrated power and the surveillance state: Chicago Chief of Detectives insider information used for thefts (at least $5M) (RISKS 21 73)

• A software failure resulted in 50 German phone-tapped suspects being billed for eavesdropping connections, compromising the secrecy of the taps; almost 20,000 lines currently under surveillance in Germany (RISKS 22 33)

* Yugoslav forces intercepted unencrypted NATO air communications during the recent war, and thwarted attacks (RISKS 20 37)

Database Abuses

• Stalker got address of TV actress Rebecca Schaeffer from Calif DMV DBMS, and murdered her, July 18, 1989; new regulations on DB access: notify interrogatee, then delay response for two weeks (RISKS 9 18)

• Arizona ex-law-enforcement officer tracks down and kills ex-girlfriend; GAO report on NCIC itemizes that and many other flagrant misuses

• Woman shot by former classmate who used Internet broker to gain information (RISKS 22 46)

• Man allegedly stalks ex-girlfriend with help of GPS (SmartTrack?) under her hood (RISKS 22 46)

* NY police chief indicted for misuse of confidential database

* 3 police officers sentenced for misusing Police Nat'l Computer

Other Identity and Privacy Related Risks

There are numerous other risks in addition to the risks of identity theft. These include Character Assassination, where someone in possession of a little knowledge about you can plant misinformation and seriously damage your reputation, especially if done anonymously. Blackmail is a standard problem, but computer systems and the Internet can increase the risk of exposure and the risk of not being able to identify and apprehend the culprit.

Spamming

Spamming (the dissemination of unwanted, unsolicited, and often highly undesirable electronic mail) is particularly offensive as a violation of privacy, and dealing with it can be enormously time consuming and counterproductive. Various anti-spam techniques (SpamAssassin, ...) can thus be considered as privacy-enhancing tools — although their effectiveness is always in question, either because they block content that you want to receive, or because they do not block content you do not want to receive.

Many Internet Service Providers and system administrators resort to filtering in attempts to limit the amount of spam as well as the presence of pornography, hate material, and other offensive content. However, overzealous filtering can also represent a privacy problem, because the interposition of an institutional filter gives the institution the ability to look at everything you are doing.

Privacy Laws

There are extensive books and reports relating to privacy laws in the United States and other countries. Of particular relevance are the books published by the Electronic Privacy Information Center in Washington DC. Perhaps most important to this study is the latest EPIC report "The Privacy Law Sourcebook 2002: United States Law, International Law, and Recent Developments" noted in the bibliography below. Its Table of Contents suggests the highly relevant scope of this book:

Defining Privacy
Models of Privacy Protection
The Right to Privacy
The Evolution of Data Protection
Oversight and Privacy and Data Protection Commissioners Transborder Data Flows and Data Havens
THREATS TO PRIVACY
The response to September 11, 2001
Identity Systems
Surveillance of Communications
Audio Bugging
Video Surveillance
Satellite Surveillance
Electronic Commerce

Public Records and Privacy, Public-Private Ventures
Digital Rights Management
Authentication and Identity Disclosure
Spy TV: Interactive Television and “T-Commerce”
Genetic Privacy
Workplace Privacy
COUNTRY REPORTS from 53 countries (including Japan)

Conclusions

Within the limits of this report, we have really just begun to scratch the surface of what is becoming an enormous set of problems related to privacy throughout the world. Recognition and understanding of the privacy problems and the risks that result from inadequate action are absolutely essential. In many cases, proactive establishment of aggressive privacy policies and regulations is necessary and crucial. Waiting until serious problems become endemic is not a wise strategy and can lead to privacy disasters with potentially enormous consequences to government, businesses and other organizations, individuals, and even critical infrastructures.

This report has been prepared by Lauren Weinstein and Peter Neumann.

Lauren Weinstein
lauren@pfir.org or lauren@vortex.com or lauren@privacy-forum.org Tel: +1 (818) 225-2800
Co-Founder, PFIR - People For Internet Responsibility - http://www.pfir.org Co-Founder, URIICA - Union for Representative International Internet
Cooperation and Analysis - http://www.uriica.org
Co-Founder, Fact Squad - http://www.factsquad.org
Moderator, PRIVACY Forum - http://www.vortex.com
Member, ACM Committee on Computers and Public Policy

Peter G. Neumann
neumann@pfir.org or neumann@csl.sri.com or neumann@risks.org Tel: +1 (650) 859-2375
Principal Scientist, Computer Science Laboratory,
SRI International, Menlo Park, California 94025-3493, USA Co-Founder, PFIR - People For Internet Responsibility - http://www.pfir.org Co-Founder, URIICA - Union for Representative International Internet
Cooperation and Analysis - http://www.uriica.org
Co-Founder, Fact Squad - http://www.factsquad.org
Moderator, RISKS Forum - http://risks.org Chairman, ACM Committee on Computers and Public Policy Contributing Editor, Communications of the ACM U.S. General Accounting Office Executive Committee on
Information Management and Technology
U.S. National Science Foundation Computer Information System
and Engineering Advisory Council
http://www.csl.sri.com/neumann

Selected Bibliography

Phil E. Agre and Marc Rotenberg, editors "Technology and Privacy: The New Landscape", MIT Press, Cambridge, Massachusetts, 1997.

Whitfield Diffie and Susan Landau,
"Privacy on the Line: The Politics of Wiretapping and Encryption", MIT Press, 1998.

EPIC, "Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls", 2001. http://www.epic.org/bookstore/filters2.0/ A collection of essays, studies, and critiques of Internet content filtering. These papers are instrumental in explaining why filtering threatens free expression.

EPIC and Privacy International, "Privacy & Human Rights 2002: An International Survey of Privacy Laws and Developments", EPIC 2002. http://www.epic.org/bookstore/phr2002/ . This survey reviews the state of privacy in over fifty countries around the world. The survey examines a wide range of privacy issues including data protection, telephone tapping, genetic databases, video surveillance, location tracking, ID systems and freedom of information laws. [From EPIC Alert 10.02] This book is vii+392 pages long, and is an amazingly valuable reference work.

Harry A. Hammitt, David L. Sobel, and Mark S. Zaid, editors, "Litigation Under the Federal Open Government Laws 2002, Covering the Freedom of Information Act, The Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act", EPIC Publications, 2002.

Doug Isenberg, "The GigaLaw Guide to Internet Law", Random House 2002. http://www.epic.org/bookstore/powells/redirect/alert1002.html . In this comprehensive guide, Isenberg succinctly covers every aspect of Internet law — from intellectual property, free speech, and privacy to contract and employment law — in a concise and non-"legalese" style. His coverage provides the reader with realistic and business-oriented solutions to the most common problems relating to conducting online business in America, and is especially aimed at policy makers, researchers, company lawyers and decision-makers. Although the book is not particularly consumer-oriented, it offers a good outline of current privacy issues and raises the average reader's awareness on some of today's most important privacy risks when surfing or expressing oneself on the Internet. [From EPIC Alert 10.02]

Wayne Madsen and David Banisar, "Cryptography and Liberty 2000: An International Survey of Encryption Policy", EPIC, 2000 (http://www.epic.org/crypto&/). EPIC's third survey of encryption policies around the world. The results indicate that the efforts to reduce export controls on strong encryption products have largely succeeded, although several governments are gaining new powers to combat the perceived threats of encryption to law enforcement.

Peter G. Neumann, "Computer-Related Risks", Addison-Wesley, 1995, ISBN 0-201-55805-X. A Japanese translation also exists, Addison-Wesley, 1999, ISBN 4-89471-141-9.

Marc Rotenberg, editor, "The Privacy Law Sourcebook 2002: United States Law, International Law, and Recent Developments," EPIC 2002. (Includes the EU Data Protection Directive and the initial WP29 report on authentication services) (http://www.epic.org/bookstore/pls2002/).

Bruce Schneier and David Banisar, "The Electronic Privacy Papers", John Wiley and Sons, New York, 1997.

U.S. General Accounting Office, "Identity Fraud: Prevalence and Links to Alien Illegal Activities", GAO-02-830T, June 25, 2002 (www.gao.gov). Although this report has a specific application in mind (alien activities), it is also useful as a general reference.

U.S. General Accounting Office, "Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards, GAO-02-352, May 31, 2002 (www.gao.gov).

U.S. General Accounting Office, "Using Biometrics for Border Security", GAO-02-952, 2002 (www.gao.gov). Although this report has a specific application in mind (border security), it is also useful as a general reference, outlining strengths and limitations of each of the various competing biometric technologies.

Appendix: Glossary of Terms Used in This Report

NOTE: The terms discussed here appear in an order logically related to their dependence on one another. In general, subsequent definitions depend on previous ones. For convenience of the reader, we also provide an alphabetical summary of the included terms, and their numerical order in the glossary.

7. Alias
2. Attribute
9. Authentication
12. Authentication, Attribute
11. Authentication, Identity
13. Authorization
1. Entity
6. Identification
3. Identity, Concrete
4. Identifier
8. Identifier, Anonymous
5. Identifier, Concrete
10. Identifier, Pseudonymous

DEFINITIONS:

1. Entity. The subject of concern, typically a person, computer process, computer process, computer system, network node, corporation, organization, enterprise, government agency, or other agent in some way related to information or its processing.

2. Attribute. A characteristic associated with an individual or other entity. Examples of relatively persistent personal attributes include date of birth, eye color, height, and weight — although the last two change over time mostly for nonadults. Examples of temporary personal attributes include address, employer, and organizational role. A Social Security Number (SSN) is an example of a supposedly long-lived human attribute, whereas an Employer Identification Number (EIN) is a similar number corresponding to a corporate or organizational entity. For people, some biometrics data are persistent (DNA, certain iris characteristics), whereas some change over time or can be changed (e.g., fingerprints and hair color). Attributes associated with computers include domain names, Internet IP addresses, file names, process identifiers, and so on.

3. Concrete Identity. The information that defines an entity in terms of a set of permanent or long-lived temporal attributes. The concrete identity may be a legally defined concept, such as a legally affirmed name on a person's birth certificate that can be associated with the unique combination of attributes such as the person's date of birth, place of birth, fingerprints, and DNA, and indeed the actual person. It could also be the designated identity of a computer system.

4. Identifier. An identifier purportedly identifies a distinct entity, whether a concrete person, place, or thing. For example, a person's name is often considered as an identifier, even though it may not be unique. One entity can also have multiple identifiers. Note that an identifier may be a genuine representation of a concrete identity, a particular representation (as in pseudonyms considered below), or a false representation. Note also that some attributes are sometimes considered as (supposedly) unique identifiers, such as the SSN. However, recall the case of the two James Edward Taylors assigned the same SSN, and the case of the 12 different people all using one other person's SSN, noted above; these cases remind us that a supposedly unique identifier may not actually be uniquely associated with a single entity. Automobile, accounts, and persons each have identifiers. The automobile has a license plate, and the account has a number. A person (e.g., owner, driver, system user) may be associated with either an auto or or an account through additional information, e.g., serial number, or a certificate. An automobile has a permanent vehicle identifying number (VIN) and a state-dependent license plate identifier. Unique computer-related identifiers include globally unique IP addresses and completely qualified file names within a particular system's directory hierarchy. However, note that local file names need be unique only within a particular directory.

5. Concrete identifier. Persistent identifiers associated with an individual human and the attributes that are difficult or impossible to alter, for example, a legally established name (which, however, may not be unique even if is genuine). For example, name, date of birth, height, and weight may be used in part as identifiers, although name and date of birth are relatively easy to falsify. Genetic information can also be used as an identifier, and is not easy to falsify. Within a computer system, there are system-lifetime persistent unique identifiers, for example, with embedded time-stamps,

as opposed to temporary identifiers that may be reused.

6. Identification. The association of an identifier with an individual or other entity that presents some sort of identifying attributes (whether correct or not). For example, a system accepts the given association between a physical person and a claimed identity. Note that authentication is not yet present (see item 9, below).

7. Alias. An identifier that is one among a set of identifiers, all associated with the same entity.

8. Anonymous identifier. An identifier associated without any explicit link to a specific entity, that is, without any personal identifier. An anonymous identifier is typically a single-use identifier that is not concrete. It may also be an alias that is not explicitly linked to any entity. (Note that an anonymous identifier used more than once becomes a pseudonymous identifier.)

9. Pseudonymous identifier. An identifier associated with attributes or sets of transactions, but with no concrete identifier and no explicit correspondence with any entity. Pseudonyms may change over time or may be persistent.

10. Authentication. Demonstrating an affirmed association between an identifier and an entity, with some hopefully nontrivial assurance. In general, a password or cryptographically generated token is used to provide some level of assurance that the authentication is valid. Similarly, the driver of an automobile is authenticated based on a driver's license bearing a recognizable photo and possibly a fingerprint, sometimes accompanied by check of the law-enforcement databases. The identity of an automobile is authenticated as legitimate by the combination of the license plate, a supposedly nonforged vehicle registration, and a check of the registration and vehicle identification number with the database of vehicles to ascertain that the vehicle is not stolen.

11. Identity Authentication. Demonstrating an association between an entity and an identifier. For example, the association of a person with a credit or educational record. This is usually a two-step process, where first identification is established, and then the link to identification and claimed attribute is established.

12. Attribute Authentication. Demonstrating an association between an entity and an attribute. For example, the association of a painting with a certificate of authenticity. Again this is usually a two-step process, where the association between entity and identifier is established, and then the link to the identifier and attributes is established.

13. Authorization. A decision to allow a particular action based on an identifier or attribute. Examples include the ability of a person to make claims on lines of credit; the right of an emergency vehicle to pass through a red light; certification of a radiation-hardened device to be attached to a satellite under construction; the privilege of a particular user or system to use a particular program, data file, or network resource.

[NOTE: This list is based in part on deliberations of an ongoing discussion group, identity@ksglist.harvard.edu, created by Jean Camp, jcamp@camail1.harvard.edu, at Harvard's University's John F. Kennedy School of Government.]

Addition: Specific Tech Issues
compiled by Cameo Wood

UUDI is an established XML business registry designed for business to exchange information, find an appropriate services and to interact with that service. The main development site for this technology is the Oasis UDDI resource website, featuring white pages updates on current development. XML has become a valuable mechanism for data exchange across the Internet. SOAP, a means of sending XML messages, facilitates process intercommunication in ways not possible before, while UDDI seems to be fast becoming the standard for bringing together providers and users of Web services; the services themselves are described by XML in the form of WSDL, the Web Services Description Language.

The other area of rapid growth is that of security. Traditional methods of establishing trust between parties aren't appropriate on the public Internet or, indeed, on large LANs or WANs. Trust mechanisms based on asymmetric cryptography can be very useful in such situations, but the ease of deployment and key management, the extent of interoperability, and the security offered are, in reality, far less than the enthusiastic vendors of different Public Key Infrastructures (PKI) would have us believe. There are particular difficulties in dealing with hierarchical data structures and with subsets of data with varying requirements as to confidentiality, access authority, or integrity. In addition, the application of now standard security controls differentially to XML documents is not at all straightforward.

Several bodies are actively involved in examining the issues and in developing standards. The main relevant developments here are XML encryption and the related XML signature, eXtensible Access Control Language (XACL), and the related Security Assertion Markup Language (SAML — a blending of the formerly competing AuthML and S2ML). Each of these is driven by OASIS, and XML Key Management Specification (XKMS).

In part because the standards are still developing, the number of toolkits and libraries available to developers are still limited, although this is certainly beginning to change. IBM has submitted two relevant Java Specification Requests (JSRs) to the Java Community Process (JCP). These are JSR-105, XML Digital Signature APIs, and JSR-106, Digital Encryption APIs.

The IBM Tokyo Research Laboratory developed the XML Security Suite in 1999 as a prototype implementation of XML signature. It contains utilities that automatically generate XML digital signatures, implement the W3C's Canonical XML working draft, and provide element-level encryption through an experimental implementation of XML encryption. It also provides a means of dealing with the particular requirements of security as they apply to XML documents. The XML schema definition of the eXtensible Access Control Language (XACL) is also introduced.

Infomosaic has produced SecureXML, the first C-Language implementation of the W3C XML Digital Signature standard. Its small and highly optimized code size makes it most appropriate for high volume XML transaction applications. The SecureXML Digital Signature is available as a C-Runtime Library, ActiveX COM Object and in the SecureXML Signature Verification Web Service.

Microsoft.s .NET framework was designed from the ground up to support XML Web services, a model for distributed computing in multiple environments based on standard protocols such as XML, SOAP, and HTTP. XML Web services can be used to integrate applications running on different platforms, or to offer software as a service.

RSA BSAFE Cert-J is RSA Security.s certificate handling software developer kit (SDK) for creating applications that integrate into a public key infrastructure (PKI). Based on open standards and thoroughly tested for multi-vendor interoperability, RSA BSAFE Cert-J provides in one package all the certificate processing and cryptographic software that developers need for building PKI-enabled applications in Java.

Baltimore's flexible approach to toolkits means that KeyTools XML can use any JCE/JCA (Java Cryptography Extension / Java Cryptography Architecture) compliant cryptographic provider (including Sun's native JCE provider) or Baltimore's own JCE provider (KeyTools Pro). Full PKI support is provided, including certificate revocation list (CRL) support and On-line Certificate Status Protocol (OCSP) support.

SAML is an imitative driven by OASIS that attempts to blend the competing specifications AuthML and S2ML, and to facilitate the exchange of authentication and authorisation information. Closely related to SAML, but focusing more on a subject-privilege-object orientated security model in the context of a particular XML document, is the eXtensible Access Control Markup Language, also directed by OASIS and variously known (even within the same documents) as XACML or XACL. By writing rules in XACL, a policy author can define who can exercise what access privileges for a particular XML document, something relevant in the situations cited earlier.

XKMS, now being considered by a W3C committee, is intended to establish a protocol for key management on top of the XML signature standard. With SAML, XACL, and

other initiatives, XKMS is an important element in the large jigsaw that makes up security as applied to XML documents. Its immediate effect is to simplify greatly the management of authentication and signature keys; it does this by separating the function of digital certificate processing, revocation status checking, and certification path location and validation from the application involved — for example, by delegating key management to an Internet Web service.

OpenSAML has been produced by Internet2 members as part of their work on the Shibboleth project. OpenSAML is a set of open-source libraries in Java and C++ which can be used to build, transport, and parse SAML messages. OpenSAML is able to transform the individual information fields that make up a SAML message, build the correct XML representation, and unpack and process the XML before handing it off to a recipient. OpenSAML fully supports the SAML browser/POST profile for web sign-on, and supports the SOAP binding for exchange of attribute queries and attribute assertions. It does not currently support the browser/artifact profile or other SAML messages involving authorization decisions.

The Privacy Rights Clearinghouse http://www.privacyrights.org/

The Electronic Privacy Information Center (EPIC) http://www.epic.org

U.S. Federal Trade Commission's privacy page

The Global Internet Liberty Campaign's Privacy and Human Rights http://www.privacyinternational.org/survey/

Protocol Issues:

The Platform for Privacy Preferences Project (P3P) is an emerging industry standard that enables web sites to express their privacy practices in a standardized format that can be automatically retrieved and interpreted by user agents. The goal is to help users be informed about web site practices by simplifying the process of reading privacy policies. With P3P, users need not read the privacy policies at every site they visit; instead, key information about what data is collected by a web site can be automatically conveyed to a user, and discrepancies between a site's practices and the user's preferences can be automatically flagged. The goal of P3P is to increase user trust and confidence in the Web.

Although P3P provides a technical mechanism for helping inform users about privacy policies before they release personal information, it does not provide a mechanism for ensuring sites act according to their policies. Products implementing the P3P specification may provide assistance in that regard, but that is up to specific implementations and beyond the scope of the specification. P3P is intended to be complementary to both legislative and self-regulatory programs that can help enforce web site policies.

Group signature schemes are a relatively recent cryptographic concept introduced by Chaum and van Heyst in 1991. In contrast to ordinary signatures they provide anonymity to the signer, i.e., a verifier can only tell that a member of some group signed. However, in exceptional cases such as a legal dispute, any group signature can be "opened" by a designated group manager to reveal unambiguously the identity of the signature's originator. At the same time, no one — including the group manager - can misattribute a valid group signature.

Zero-knowledge protocols allow identification, key exchange and other basic cryptographic operations to be implemented without leaking any secret information during the conversation and with smaller computational requirements than using comparable public key protocols. Thus Zero-knowledge protocols seem very attractive especially in smart card and embedded applications.

Digital Privacy Rights Management Mechanisms and Digital Rights Management

Divx was the first consumer product based on controlled use of digital content. Its cancellation suggests that while the technology is promising, there are a number of issues left in designing digital property right management systems that will have widespread success in the consumer market.

Internet-based distribution of mass-market content provides great opportunities for producers, distributors, and consumers, but it may seriously threaten users' privacy. Some of the paths to loss of privacy are quite familiar (e.g., mining of credit-card data), but some are new or much more serious than they were in earlier distribution regimes. Privacy-enhancing technology (e.g., encryption, anonymity, and pseudonymity) absorb most of the attention of the security R&D community, and cannot by itself solve the privacy problems raised by DRM, although it can play a role in various solutions.

In addition to preventing anonymity in access to digital information, DRM can be used to facilitate profiling of users' preferences or to limit access to certain content. This is done by assigning an identifier to content or to the content player, and attaching personal information to the identifier. For instance, Microsoft's Windows Media Player has an

embedded globally-unique identifier (GUID) to track users. Similarly, Microsoft's eBook Reader requires the user to "activate" the software and link it to a Passport account. From there, Microsoft captures a unique hardware identifier of the user's computer. There is also an activation limit that can stop a user from transferring an eBook to other computers. This enables Microsoft to prevent users from sharing books or from reading a book on a different machine.

Also, Windows Media Player creates a log file of the content a user views, and "phones home" to a central server to obtain content titles. These technologies mark an important development in the use of copyright law: copyright can regulate duplication of works to protect content owners. Now, copyright is being used as a justification to both protect content and to profile the consumers of content.

Linking personally-identifiable information to content may result in "price discrimination." Price discrimination is the practice of selling an item at different costs to different consumers. It can be facilitated where the seller knows the consumer's identity, and can associate the identity with a profile that includes financial information on the consumer. DRM systems may enable content owners to control access to content, but also to adjust the price of content based on the consumer's identity.

Alternatives exist that would provide copy protection and at the same time protect privacy. For instance, token and password systems could be used to authorize a download of digital content. Alternative, non-privacy invasive solutions have not been explored adequately.

Many DRM systems will not allow a user to transfer content to portable devices, such as MP3 players. In addition, many DRM systems work only with Windows operating systems to the exclusion of Linux and Macintosh users.

Anti-Traffic analysis techniques

Aesop (Advanced Encrypted Stackable Open Proxy) is a TCP-proxy which tries to safeguard your privacy and anonimity. Aesop combines a fast and reliable TCP-proxy with strong cryptography and a full scala of anti-traffic-analysis techniques. These techniques include stacking multiple proxies in a chain, stream multiplexing, random padding, random packet injection, constant transmission speeds, etc.. Despite all these complex capabilities usage of aesop is transparent to the user while it stays very flexible and configurable for the power-user. Aesop ships with a preloadable library (libaesop) which can be used to make almost every network application go through aesop. Further, aesop is written with security in mind and reasonably lightweight.

PKI . public-key infrastructure.

PKI enables individuals to encode messages and transmit them so that only the proper recipient can receive and decode them.

Although not an exhaustive list, here are a few examples of real world PKI solutions:

Singapore, Finland — PKI for national ID

Australia, Ireland - PKI for secure tax filing

NATO — PKI to support electronic procurement

Canadian Department of Defense — PKI for accessing and communicating sensitive information

Canadian Government - PKI for secure government-to-citizen transactions

Wells Fargo Bank, Robobank, Identrus, Visa International, Canadian Payments Association, United States Department of Defense - PKI for supporting secure e-business

Johnson & Johnson — enterprise PKI to support operating companies, external contractors, partners, and customers

Fannie Mae — PKI for secure loan processing

Viacode — PKI for Identification

Phyve, Kaiser Permanente - PKI for secure medical solutions

Addition: Use Case of Electronic Voting and its voter privacy protection method *compiled by Cameo Wood*

The FVAP VOI Pilot Test

http://www.fvap.gov/voireport.pdf

In November 2000, the Federal Voting Assistance Program (FVAP), an agency of the American Defense Department, executed their first Voting over the Internet (VOI) Pilot Program. Eighty-four residents living abroad (officers of Air Force, Navy, Army, Marines, CoastGuard). Voters were chosen from 21 states and 11 countries including Weber County, Utah, the State of South Carolina, Dallas, Texas, Orange and Okaloosa Counties. This was the first time that online voting was used for a local, state and federal election.

The Secretary of Defense is the presidential designee for administrating the federal provisions of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986 that covers the voting rights of all members of the Uniformed Services, the merchant marine, and their family members, federal employees overseas civilian citizens not affiliated with the Federal government.

The secretary responsible for elections in Okaloosa County reported that of over the 496 initial respondents citizens, 139 were eligible at voting time, 91 were registered for the VOI and 84 voted. These 84 e-votes came from 28 States and territories, 12 countries (Europe, Middle East, Far East).

The FVAP was responsible for the installation, testing and training on the hardware and software necessary for the pilot project at the Local Election Offices. To achieve this election through the Internet, the FVAP contracted BoozAllen Hamilton to develop the software. FVAP.s Defense Department connection allowed them to use the military Internet system, as well as their security (encryption, digital certificates, etc).

The most important design elements in the architecture of this system were designed to be as similar to the existing physical ballot system as possible. Security, secrecy, and transparency of the electronic voting process were the most critical aspects considered in the design.

The ways in which a voting system is measured by the government in accord with privacy rights in the US Constitution is as follows: Only people who are entitled to vote can vote; Nobody can vote twice or in another person.s name (unless an authorised proxy); No votes are lost or duplicated in the process; How an individual vote was cast is secret; The votes cast remain secret while the vote is in progress; There is an audit trail to enable the detection of fraud; The electoral process is protected against interference and corruption; and There is no disruption through a failure of infrastructure.

Each of the five jurisdictions that participated in the project had their own Internet provider. The Local Election Office administered the system and processed voting materials. The FVAP provided a central server for the secure transmission of voting materials from citizens to local election officials and vice versa. The server maintained an audit trail of all transmissions but did not store voter information in an unencrypted form. For further protection, LEOs maintained two-person control of the private key of the privacy certificate. Because one official knew the password and the other official had physical control of the digital certificate, one official could not decrypt ballots without the interaction of the other official.

FVAP solicited Volunteers from all the Uniformed Services. All potential volunteers had to meet the UOCAVA absentee voting requirements of one of the participating jurisdictions and have access to an IBM-compatible PC and the Internet. A .Citizen Information Packet. was provided containing the citizen.s software with complete instructions on how to load it and use the pilot system. Once the citizen connected to the FVAP network, he or she only needed to follow the instructions on the screen.

The Department of Defense sent volunteers Public Key Infrastructure certificates via the postal mail, which then had to be registered at a local physical office. The certificates were used to identify them to the Federal Voting Assistance Program server and submitted a digitally signed, completed electronic Federal Post Card Application which was then forwarded directly to the Local Election Office Server. Once the ballots were available and the citizen requested a ballot, the Local Election Office Server transmitted an electronic version of the appropriate ballot through the FVAP Server to the citizen.

FVAP.s security was based upon the physical traceability and redundancy of postal mail, access control lists, intrusion detection systems and a .secure operating system configuration.. The voted electronic ballot information was encrypted and sent through a Secure Socket Layer. The VOI system was equipped with filtering routers, Intrusion Detection Systems and specially configured operating systems to safeguard unauthorized system penetration. All data transfers associated with the pilot used the SSL protocol.

The VOI system gave self-tests to verify that the secrecy of the ballot was maintained. Secrecy of the ballot means that no one can connect a voter.s identity with the contents of his/her ballot. The government report stated, “secrecy helps

facilitate freedom of choice by discouraging direct and indirect coercion in voter selections."

To maintain the secrecy of voted ballots, the LEO server separated the digital signatures from the voted E-Ballots before they were decrypted and printed. The ballot processing software on the LEO server randomized the ballots after the signatures were removed and before they were printed, so that a printed E-Ballot could not be linked by order to a voter. This process provided a high level of secrecy protection for VOI Pilot voters. Independent testing showed the VOI System passed 100 percent of the transmission confidentiality tests. Testing also showed that in all cases, E-Ballot processing removed the links between voter identity and the E-Ballot choices, maintaining the secrecy of the ballot.

The VOI System was designed to maintain detailed transaction logs of System events to facilitate post-election audits and recounts. For example, VOI System transaction and security logs recorded all citizen log-ins, all EFPCA or E-Ballot requests and submissions, all Status Check requests, all denied requests for materials, and all instances in which the LEO server was not responding. The logs could be queried by different variables, such as the user common name, which allowed administrators to review the activities of a specific VOI user or time period. The system administrators could then reconstruct activities during a given period of time.

In conclusion, the voting system was well intentioned and designed under appropriate guidelines, but the complexity of Digital certificates and the physical duplication of votes made the system very cumbersome. Also, because votes could potentially still be traced back to an individual user, this system does not properly protect the privacy rights of the voter, making it unsafe.