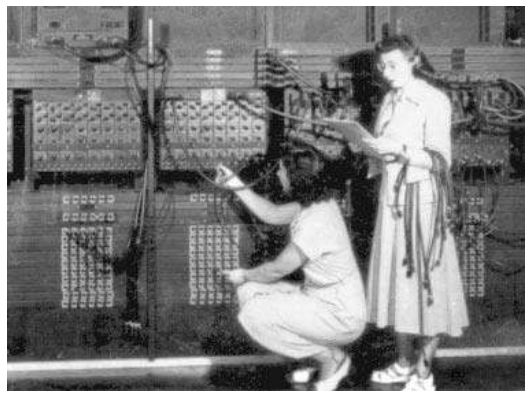
Miscellaneous Surveillance

18

Computers



1. Introduction

Computers are changing the surveillance industry in many important and dramatic ways. There are three aspects of computers that make them particularly suitable for surveillance tasks. They can automate surveillance devices, they can quickly process data in ways that are not otherwise possible, and they can be interconnected to share information. *Computer network surveillance* involves administering and monitoring a network, functions that are handled by experts and not covered in this introductory text. *Computerized surveillance*, using computers to control electronics and process data gathered from a variety of sources, is becoming extremely prevalent and is carried out by people with skills ranging from novice to expert.

Computers have spread into many aspects of western life, causing a dramatic shift in information access and technological capabilities. Ten years ago, it wasn't possible for private citizens to look up the name, address and phone number of a person hundreds of miles away. Even if they called Directory Assistance, the addresses in the phone directory weren't given out by the phone company, only the phone number. Reverse directories were very hard to find. Now there are half a dozen reverse directory sites available to anyone with a computer and an Internet connection with access to the World Wide Web.

Programmers rewiring the ENIAC computer in 1946. [U.S. Army historical photo, public domain.]

Fifteen years ago, the average citizen couldn't lay out and print a publication-quality manuscript. Now, with desktop computers and laser printers, many people have this technological capability. Thus, computers allow many tasks to be carried out at home that were previously contracted out to professionals.

These dynamics are creating an increase in the volume of surveillance information that is available and a shift in the accessibility of this information. New categories of people are being attracted to the surveillance field by the capabilities of computers and existing surveillance professionals may have to reinvent their roles, shifting from 'insiders' and 'information hunters' to consultants and information organizers and brokers. This chapter introduces some of the more common ways in which computers are used to conduct surveillance and to process data from other types of surveillance devices.

The Power of Networking

Computer networks provide far more information than many people realize. There is so much information, in fact, that it is possible to profile the lives, preferences, and personal habits of tens of thousands of people who don't even have computer access and who may never have logged onto the Internet. As a result, detectives, advertisers, business competitors, and individuals seeking family members or old friends regularly use the Internet to seek out people, companies, products, and to monitor news and activities around the world.

There are two primary sources of network intelligence at this time: the *Internet* and *local area networks* (mainly in the workplace). With more than 40 million people regularly connected to each other on the Internet in one way or another, the amount of information that is shared and that can be gleaned from the Net is orders of magnitude greater than what can be derived from local networks (though these are still important sources of corporate intelligence). The impact of this information exchange will probably be greater than anyone has predicted and we will see its effects unfolding for many years in the future.

Surveillance through computer networks, whether global or local, is prevalent and, in many cases, does not require sophisticated tools. Computer surveillance is used for many legitimate purposes, for many marginal or gray area targeting purposes, and for many illegal or unethical purposes. Network surveillance techniques are regularly used to log project activities for later billing or evaluation, and to find people, including adoption families, lost relatives, old high-school friends, deadbeat parents, criminals, potential customers, and payment skippers. They are used as intelligence-gathering tools by a wide variety of people including private detectives, corporate and government spies, law enforcement agents, social services workers, charity organizations, stalkers, smugglers, thieves, and illicit dealers.

Information Sources

This chapter describes some of the strategies, techniques, software, and online tools that are used to locate information using computers that are integrated into networks. It emphasizes Internet surveillance and workplace surveillance, the two most common sources of surveillance information.

It further focuses on those aspects of networking that use commonly available applications. This chapter is not a tutorial on how to use the Internet. It assumes that you have mastered the basic skills of logging on, running a browser, and doing a basic search on one of the major search engines. If you do not already have these skills, there are hundreds of books that cover the basics and it only takes a few days to get some of the essential skills needed to run a browser program and conduct Internet surveillance. The best way to get started is to have someone patient and experienced looking over your shoulder and helping you for a couple

of hours. This hands-on help equates to about four days of reading and trying to figure it out on your own. Don't get discouraged if you don't have someone to help you, however. Many people have taught themselves computer skills from books and tapes and these are readily available at local bookstores and mail order outlets.

If you are just curious about network surveillance, you can enjoy the introductory descriptions, history, and sample commercial products described in this chapter without worrying too much about details, but if you are a surveillance professional doing work outside your local area and you haven't yet learned to search on computers, it is recommended that you take the time to learn. These days trying to conduct a surveillance-related business without computer skills is like trying to publish a book with a pen instead of a word processor. The old ways of conducting surveillance are not obsolete, but they are no longer complete.

2. Types and Variations

Basic Terms and Concepts

Here are some of the most basic terms and concepts related to networking that will aid in understanding the contents of this chapter. (A few more can also be found in the Glossary at the end of the chapter.) The more technical terms (and network topologies) have been deemphasized, to keep this chapter as straightforward and user-oriented as possible. If you have a technical background, you should seek out specialist sources. If you are just becoming familiar with computers, this chapter will help you get started.

Here are some of the most common terms associated with computer surveillance organized conceptually, rather than alphabetically:

network - two or more computers with a communications link between them

intranet - an internal network as would be found in an office or a school

internet (with a small 'i') - networks joined externally, such as those in separate buildings

Internet - a worldwide network of thousands of computers all linked together through wired and wireless connections, routers, and servers.

World Wide Web, the Web, WWW - a somewhat self-contained client-server software interface/environment that is a subset of the Internet. The Web supports graphics, files, text, and other structures that provide document display and simple user interactions mainly through a markup language called *HTML*.

Web browser - a software applications program which interacts with a Web server to allow a user to access Web-compliant files on the World Wide Web. To most people using common browsers, the Web appears as a graphical (or text) window within their computer desktop environment.

Web browser plugin - a third party software program that works in conjunction with a Web browser to provide added capabilities, usually graphics, sound, and animation programs. Web browsers (and servers) are evolving to support technologies that are conceptually similar to interactive television. Plugins serve to extend the technology while allowing browsers to remain essentially the same, resulting in a modular approach to providing content on the Web.

cookie - a software marker or identifying piece of information that may potentially be accessed by other computer programs. Browser cookies are sometimes used by Web vendors to streamline customer service and purchasing functions. In most cases, a cookie can be disabled in order to safeguard privacy, though there is nothing right

now that stops a large (or small) vendor from hiding cookies in their commercial applications programs and not telling their customers about their presence. When this happens the computing community usually hears about it from watchdog agencies before the vendor admits to the fact.

back door - a means of accessing a software program that is intentionally (and usually clandestinely) left by the programmer. It will never be known just how many back doors there are in computer software, as they can be difficult to detect. Some are there for legitimate reasons, for allowing the programmer or network manager to quickly access a program for maintenance or troubleshooting; others are there so that unethical or disgruntled employees or ex-employees can access the program or system without the knowledge of others.

search engine - a software program that allows you to enter keywords, titles, or concepts in order to search and retrieve information from one or more archives. There are about a dozen prominent search engines on the World Wide Web.

firewall - a type of data security system designed to keep certain users or data out (or in). For example, a classroom or corporate network which is connected to the Internet may have a firewall to prevent outside Internet users from accessing the school computers. A secure firewall may even prevent outside users from being able to easily detect the presence of the school system on the Internet.

router (or *switcher*) - an electronic peripheral device which controls or aids in controlling the flow of data traffic in a network. Switchers are becoming so sophisticated that there is a lot of overlap between routers and switchers and the distinctions between them are disappearing. Routers range from simple consumer routers for managing traffic between a few machines to *routing distribution networks*, city-block-sized buildings with tens of thousands of connections.

media space - an environment wired with media connections, usually video and sound, in order for the space to support communication or collaboration between individuals in different locations. Media spaces are used to facilitate remote communication between workplace departments, different company branches, collaborating businesses, and teleworkers. Videoconferencing is commonly used in media spaces.

3. Context

The Internet Versus The Web

One of the most important concepts to grasp in computer network surveillance is that the Internet and the World Wide Web (WWW) are not the same thing.

A *Web browser* is a software tool that displays information dispensed by *Web servers*. Imagine going to a food complex with a dozen restaurants offering food ranging from fast food to fine dinners. The various kitchens are full of ingredients, cooking equipment, and chefs who are capable of providing a vast number of meals, but there are no signs or menus. Experienced patrons know the best chefs and can walk into the back rooms and let them know which meals to prepare. However, this is logistically difficult for first-time visitors or people without a culinary background. The Internet is similar to a food complex with no signs or menus. There are a lot of people behind the scenes, many resources, and there could be many more meals cooked from the basic ingredients than people actually order. Experts could come into the food court and pick a chef and a group of ingredients and ask for custom meals.

However, most visitors to the food court would be too inexperienced and too shy to ask for custom meals, and many would be just too busy to wait.

The Internet is somewhat like the unadorned food complex without waiters or menus. It has a wealth of resources that experts can readily use, but is confusing for people without computer expertise. There are strange codes, unfamiliar procedures, and hundreds of commands. Along comes a menu system. By organizing some basic dishes and putting up colorful billboards, the restaurants in the food complex can immediately advertise their style of food and the various meals that are available to the general public. The Web provides a similar means of presenting goodies on the Internet. The World Wide Web is a system of dispensing information about what is available in a readily accessible form so the average person without a technical background can access the resources. Just as a restaurant can hire waiters to present menus and information on daily specials, a *Web server* can dispense information on the various resources that are on the Internet in Web format. Just as a restaurant patron uses his eyes and ears to read the menu and listen to the specials, the *Web browser* provides an interface that allows a computer to display the various sights and sounds on the Web that are 'served up' to the browser. This is called a *client-server* system.

Thus, the Web is only a subset of the Internet. In fact, five years ago it was a very tiny subset of the Internet, but over time, it has grown. The Web doesn't let you see the whole Internet, it doesn't let you talk directly with the people behind the scenes, and it is a somewhat prepackaged environment compared to the Internet as a whole, but it is colorful, sometimes relevant, dynamic, and much easier to use for people who don't have a background in computers. Most of the Web is point-and-click. In other words, if you can use a pointing device like a mouse, you can use the Web.

As far as surveillance is concerned, there are thousands of data repositories which are not Web-accessible, or which are indirectly Web-accessible, that are important information sources. There are also thousands of newsgroup feeds and dozens of realtime chat and email discussion lists that are not necessarily listed or directly accessible via the Web. This is gradually changing, as the Web evolves and programmers get better at integrating Sun Java™ routines into Internet browsers, but at the present time, it is important to note that you need a variety of techniques to access the many sources of public information.

Since this is an introductory text, it concentrates on readily accessible Web tools. For delving deeper into the Internet, it is recommended that you learn some *command line* skills and *UNIX* skills from some of the many good books that are available. Then you can go in the back room called the Internet, and order your own custom meals.

Search in the Broader Context

The single most important skill that a surveillant using the Web needs to acquire is the ability to use search engines effectively. A search engine is a tool for finding specific types of Web pages. There are more than a billion pages on the Web, and there is no easy way to reach them without using a search engine. If you are looking for sites that list names and addresses, a Web search engine can pick out the relevant sites and list them for you with a short description. With practice, it's possible to use search engines in such a way that you narrow down your search to a few hundred or a few dozen of the best sources.

First you need to understand Uniform Resource Locators (URLs). In simple terms, these are Web addresses. Just as you have a house number and a phone number to identify your physical location, a site on the Web needs a URL to identify the location at which the information is stored. URLs follow standard formats. The one most relevant to this topic is the

location of a basic Web page which will look something like this:

`http://www.abiogenesis.com/surveil`

Typing this URL into a Web browser takes you to the author support site for this text. From there you can click on links to the resources listed at the back of each chapter. It will also take you to some of the major search engines on the Web.

There are hundreds of Web search engines but there are a number of particularly useful or popular sites including the following:

Name	Web Address (URL)	Notes
Alta Vista	http://www.altavista.com/	Good advanced search capabilities, large list of sites, language translation.
Ask Jeeves	http://www.askjeeves.com/	Will accept phrase and sentence queries and narrow down hits to the best choices from each source.
DejaNews	http://www.deja.com/	A good resource for word-of-mouth information. (It used to be a superb source of newsgroup dialog but is now somewhat hampered by a lot of graphics and ads.)
Entrypoint	http://www.entrypoint.com	Will email alerts and news to you based on your stated preferences.
Excite	http://www.excite.com/	General search, weather, stocks.
Google	http://www.google.com/	Good search engine with over a billion indexed pages.
InfoSeek (Go.com)	http://www.go.com/	Web pages, newsgroups, individuals.
Inktomi	http://inktomi.berkeley.edu/	U.C. Berkeley distributed database.
Lycos	http://www.lycos.com/	General search, maps, news, names.
Magellan	http://www.mckinley.com/	Reviewed and rated sites.
Sleuth	http://www.sleuth.com/	Access to Internet databases in general categories.
Starting Point	http://www.stpt.com/	Web and Internet, news, includes advanced search.
Web Crawler	http://www.webcrawler.com/	Quick, simple.
Yahoo	http://www.yahoo.com/	Organized by categories.

Sources of information on the Web are diverse and plentiful, so it is usually best to tackle information-gathering with a specific focus. Everyone is trying to hold your attention, so it is very easy to get lost or distracted while searching on the Web.

The types of surveillance-related information that can readily be found on the Web include

- the names, addresses, and phone numbers of people and businesses, particularly those who have listed numbers in North American or Western European paper directories
- personal Web pages and profiles of people who are frequent Web users
- detailed maps of roads, businesses, recreational services, and transportation systems from most communities in developed nations, particularly North America
- commercial and government satellite photographs
- environmental and geological statistics and images
- lists of library holdings and educational publication lists
- lists of business products and services
- announcements of new technologies and their inventors
- patent and trademark information, particularly those registered in the last two decades in the United States
- lists of people who have made significant achievements in sports, science, and business
- newspaper and magazine articles about specific people or technologies
- discussion groups of advocates for specific causes
- government and private statistical compilations and population demographics
- proceedings and positions of state and federal government political bodies
- unclassified activities of the armed services and White House personnel

Private detectives make regular use of the Web to locate 'skips' (people who are avoiding payment or justice), adoptees and their families, and to track the activities of individuals and corporations.

Marketing agents use the Web to plot demographics, consumer buying trends, and to assess the competition. They also amass postal and electronic mailing lists.

Entrepreneurs use the Web to assess existing patents and inventions and to determine whether other companies are already making or distributing products similar to those they are considering developing. They also use Web information to develop business plans and communicate with potential investors, employees, and business associates.

Stock investors, brokers, and venture capitalists extensively use the Web to assess market trends, business activities, new ventures, and competitive activities.

Intelligence agents use the Web to track foreign communications, to uncover crimes, to detect and apprehend stalkers, poachers, smugglers, and terrorists, and to assemble information of a general nature which might be relevant in later contexts.

Using Good Tools

An enormous amount of information can be gathered with a simple browser and a dialup Internet account, but if searching the Net is part of a professional service or task, then an up-

to-date browser and a fast-access account (T-1, DSL, ISDN, or cable modem) can save an agency, and a client, a lot of time and money. Many Web sites are now enhanced by graphics or hopelessly cluttered by them. Many now have animated ads that greatly slow down the speed at which a page will load. When downloading files or images, the difference between a fast access account and a regular modem for downloading a 10 MByte file can range from a couple of minutes to over an hour.

Privacy, Security, and Anonymity

It is not easy to remain anonymous on the Web. There are many extremely intelligent computer techies who love to solve puzzles. One of those puzzles is finding ways to detect the activity of a browser and the person using it. They have also worked out ways to get your email address. Don't believe it if someone says you don't give out personal information when using a browser if your identity is taken out and your 'cookies' disabled. If you use an email program that is built into the browser and someone sends you email with a built-in URL that you can just click instead of typing, that automated click can provide information automatically. As browsers become more sophisticated, it becomes easier to build 'smart features' into the browser that can be controlled offsite.

Many users of IBM-licensed/Microsoft-based personal computers don't even realize that when they get their DSL or cable modem linkup they are visible to other people on the Internet unless they set up their system with certain security settings or a firewall. This information can make it possible for hackers to access your files.

Browsers leave trails. If you wish to search or email anonymously (or avoid the inevitable backwash of junk email that results from leaving messages while searching the Web), you need to disable cookies, remove the 'Identity' information from your browser, use particular servers, and often set up other security. This is beyond the technical expertise of most casual computer users.

A *cookie* is a token or ID that can be passed from computer to computer or from one software process to another on one or more systems. It provides a means to keep records of processes or activities. If you regularly log onto a site such as a book store or other Web vendor, you may have noticed that they will ask if you want to be 'remembered' for subsequent transactions (so you don't have to type in your name and other information every time). This information is derived from a cookie and then is stored in the vendor's database. When you log back on to the system at a later date, the software checks your browser cookies and calls up the previously stored information, sometimes greeting you by name. Cookies are used in many Web 'shopping cart' systems. Some sites are even set up to track a browser as it leaves a site. In some cases, the remote site will deposit a *reverse cookie* on your site, which creates a security gap through which hackers could potentially compromise your data.

It is difficult to completely cover your tracks and protect your privacy online. Some individuals choose to disable the majority of identity tags in their browsers as a sort of minimal protection and leave it at that. For high security, aliases and anonymous servers are necessary to preserve privacy. An anonymous server is a system set up to forward messages without identity tags to protect the identity of the sender. For example, a frightened witness to a violent crime might send a tip to law enforcement officials through an anonymous server. A refugee from a foreign country might use an anonymous server to communicate with relatives in the home country in order not to reveal his whereabouts to a repressive government. A news journalist in a war zone might use an anonymous server to send information to his or her editor in another region. Anonymous server issues are described in more detail in specialized books on preserving privacy on the Internet.

Information-Gathering Strategy

As has been mentioned, the Internet is a big place. If you were an archaeologist who just located an ancient 15-acre underground ruin of passages in an area that was going to be bulldozed in three weeks, you would understand the importance of priorities and good searching strategies. Unless you have unlimited time and resources, it is best to approach information-gathering on the Net in the same way. A typical search for a topic on a Web search engine can yield anywhere from 8,000 to 8,000,000 'hits,' that is, sites with information pertaining to your query. It is recommended that you learn to use the Power Search features provided with every major search engine, as this will help you narrow the searches down to several hundred hits without sacrificing quality.

Decide what it is you need to know and then doggedly and patiently seek it rather than trying to see everything there is to see. There are times when a wider viewpoint is valuable, but much of the time it is best to focus clearly on a specific goal. Avoid the temptation to explore side-routes. When scanning the 'hits' that are provided by search engines, read the descriptions and select the ones that look most relevant, don't just go down through the list clicking each one unless the number of hits is small and you are having trouble finding the information you need.

The Context of the Internet

The Internet is a powerful source of information as long as the information-seeker understands the particular character of the Internet. At the present time, users of the Internet do not represent a microcosm of human society. If the world is a cake, then the Internet is not a slice of cake, but rather a spoonful of whipped cream icing.

There are many sources of information on the general population that can be found on the Internet, but not all surveillance intelligence is based on looking up names and addresses. Some of it is based on studying Web pages and articles written by the people who comprise the Net community. This is not a typical cross-section of society.

There are many research companies that have studied the demographics of the people using the Internet. They have discovered that, statistically, Internet users as a group are affluent, male, white, well-educated, young to middle-aged, and generally Libertarian in their political leanings. They have also discovered that, as huge as the Internet has become, many users are only passive listeners (called *lurkers*), browsing the Web once in a while, or private emailers, who interact exclusively with a small social group. These people leave indirect footprints on the Web. Much can still be discovered about them, but it must be done through clandestine technical surveillance or through secondary sources (which are, in fact, numerous).

The software and content providers on the Net are themselves a specialized society. Those who are the most visible and active on the Net usually have a strong technical background or a strong political agenda. Those who produce the vast majority of information and programs that define the character of the Web only represent a tiny fraction of the human population, about 0.1%. This produces a bias in the medium itself. Marshall McLuhan made a historic, often-quoted statement regarding television in the 1960s when he stated that "The medium *is* the message." The concept holds just as true today for the Net as it does for television.

Given this select group of people creating and relating on the Net, it can be seen that the opinions of people on the Internet and their behavior and demographics are not likely to represent the opinions of people as a whole. Thus, detectives and other professional surveillants who are gathering statistics and profiles on the Internet, need to be aware of the skewed distri-

bution in the following areas:

Economics - Until recently, computers were not cheap. Even now, many laptops and workstations cost several thousand dollars, three month's pay for someone earning minimum wage. While prices have dropped substantially, many people still can't afford computers or Internet access fees. Those with higher incomes are more apt to purchase and use computers and be connected to the Net.

Program Providers - The majority of programmers are male (currently around 85%) and there are indications that they write programs to reflect their personal interests and economic goals (e.g., video games). These personal and commercial leanings are apparent on the Web as well, though diversity is increasing as more people sign on.

Traditional Stereotypes - Computer network technology grew out of electronics developments from the 1940s to the mid-1970s, a time during which women were actively prevented from entering electronics related professions. Women and minorities still have difficulty getting upper level management positions in the technology industries (less than 3%). The age curve is also a factor in Internet use, many retired people don't use computers and never will, but there is also a trend for more retired people to use the Net when they are offered reading, gaming, and other recreational opportunities online. Minority populations often have less Net access due to job discrimination that results in lower incomes. As computers become cheaper and Internet connections are more broadly installed in public schools, these stereotypes should gradually diminish.

Recreation Time - In families with two working parents, men spend more time on computers while at home. This may be related to differences in personal interests generally and statistics indicating that women still handle the majority of child care, shopping, cooking, and other household chores that might take time away from computer activities in the home.

One other factor of relevance to surveillance is the tradition of women taking their husband's names when they marry and of adoptees being given the names of their adopted parents. Surveillance professionals using the Net to find female felons, skips, lost family members, or adoption families usually find it easier to locate primary source data on young to middle-aged white males than on other demographic groups. Information from city governments and community groups about property assessments, marriages, and legal proceedings are gradually becoming accessible on the Web and may make it easier to locate information on female subjects in the future.

Language Considerations

There are other aspects of the Internet which directly affect information-seekers. One of the most significant of these is that most computer applications are designed in English.

The majority of commercial computer programming languages evolved in America. This results in a certain amount of cultural-centricity in the technology. Just as most opera terms are in Italian and most ballet and cooking terms are in French, most computer terms are in English, where a large portion of the trade originates.

That is not to say computer technology is essentially American. A great deal of computer development has occurred in Europe and Asia. There is a strong interest in computer technology and mathematical algorithms in India and business owners and governments in developing nations would gladly use computers if they could afford them.

Consequently, in spite of a strong interest in computers throughout the world, Europeans generally program in English. Because Asian written languages are difficult to interpret into keyboards and computer syntaxes, many Asians also program in English. Many search engines have language translators that will translate a German, French, Italian, or Spanish Web pages into English text (some also translate other languages into English).

What this means for a surveillance professional is that if English is your primary language and you live in the United States, Canada, or the United Kingdom, you have an advantage in using the Internet.

Surveillance in the Context of the Workplace

Up to now, most of the discussion has been about Internet surveillance. However, local computer networks and computerized badges and access systems are also prevalent in workplaces that may or may not have Internet access.

Computer surveillance in the workplace takes many forms, from *access surveillance* for monitoring entries and exits, to *keystroke logging* to monitor activities on individual computers, to *tracking* an employee throughout a complex, including trips to the washroom. With the help of computers, a complete record of every person's movements is now theoretically possible.

It is easy to see how the computerization of tracking and monitoring technologies is of interest to employers. They are concerned about preventing employee malingering, gameplaying, personal emailing, fraud, and theft, all of which contribute to a loss of productivity and profits. Honest employees, on the other hand, are concerned that they are being discriminated against due to the activities of a small minority and further concerned about being surveilled and recorded without there being policies in place to allow an employee to review his or her file or to provide feedback on the manager, to correct misconceptions or errors, or to have transcripts destroyed after a reasonable amount of time.

The current workplace climate is one of increased surveillance through a variety of technologies, including entry access, electronic badge tracking, video surveillance, phone and email accounting systems, keystroke recorders, and phone call recorders. And 'workplace' surveillance doesn't just stop at the office. With many more people working from home, workplace surveillance now often includes a video camera installed in the home.

Surveys indicate more than half of employers currently use some form of electronic monitoring, with phone logging, storage and retrieval of email, and video monitoring listed as examples [AMAI 1999]. Telemarketing firms and computer software suppliers are particularly known for monitoring sales and technical support calls.

Electronic Performance Monitoring (a type of workplace surveillance) involves the use of computer technology to evaluate the speed, efficiency, and effectiveness characteristics of an employee. Since EPM occurs most frequently in jobs that lend themselves to monitoring, predominantly phone work and clerical work performed on computers, EPM is indirectly biased to monitoring women, who fill the majority of receptionist, word processing, and data entry jobs. Since managers rarely perform keyboard-intensive activities, they are less subject to this type of monitoring. As software programs become more sophisticated and able to monitor loans and brokerage transactions, which are statistically handled more often by men, the gender bias may decrease, but management biases may remain.

A number of concerned agencies have been studying workplace surveillance and have made some initial recommendations regarding legislation and corporate policies. Their rec-

ommendations include, but are not limited to, the following:

disclosure - Full disclosure must be given by the employer to the employees of surveillance device locations and operations, including the purpose of the surveillance, when it is active, how records are stored, who is authorized to see them or distribute them, how long they are kept, in what manner they are distributed outside the company, and how they are destroyed.

consent - An employee must give informed written consent for collection of or access to the employee's personal data or for covert surveillance of that specific individual, except under very exceptional circumstances related to 'grievous criminal activity.'

review - Mechanisms for employee review of his or her records must be put in place, with a process for the employee to correct incorrect information.

bias removal - In systems where human monitoring through video cameras exists, particularly if those cameras can be remotely aimed, strict guidelines as to objective and nonvoyeuristic surveillance must be established and upheld. This is to prevent reported abuses in the areas of minority prejudice, voyeuristic preference for videotaping young women, and prejudice against monitoring men and youth in high crime areas.

balance - Two-way surveillance between workers and management should be instituted. In other words, if employees are to be held accountable for their actions with respect to the employer/managers, a balancing mechanism needs to be in place to hold employers accountable for their actions with respect to employees. Many upper level managers resist the concept, thinking they should be 'above scrutiny' or somehow exempt, but given the powerful nature of surveillance data and the need for trust and collaboration between employers and employees for maximum workplace efficiency, these concerns need to be addressed and balanced for everyone's mutual benefit and for the long-term health of the company.

change of use prevention - Data collected for one purpose should not later be used for another purpose without the explicit written consent of those surveilled. In other words, information from employees collected for company demographics cannot later be used for marketing without employee consent. Similarly, cameras aimed at cafeterias or parking lots for 'safety of the employees' cannot later be used for employee evaluation, litigation, or other purposes, unless employees were informed in advance and agreed that they might be used for these purposes.

free zones - It is important to establish surveillance-free zones where worker privacy is guaranteed in order to ensure and promote trust and the emotional, mental, and physical well-being of employees.

Many workplace-related surveillance systems (phone logging devices, video cameras, magnetic access devices, etc.) are described in other chapters.

4. Origins and Evolution

When a new generic technology is invented, it may take a while before its surveillance potential is recognized and used. In the case of computers, their early development and their use for surveillance are so closely linked as to be almost inseparable. Almost as soon as computers were invented they were being used to create and break ciphers, to store information on people and governments, and to help solve problems which were related to economics, warfare, and information brokerage.

Using Machines to Gather Data

Mechanical calculating machines have existed at least since the 1600s, when inventors like Wilhelm Schickard (1592-1635) and Blaise Pascal (1623-1662) created some of the first calculators for aiding in financial transactions and tax assessments.

The use of mechanical calculators for the large-scale collection of information on people began with Herman Hollerith's (1860-1929) invention of a tabulating machine for counting national census data. In a sense, this was the beginning of the computer database, foreshadowing one of the uses for which computers would be adapted 100 years later. The Hollerith machine could read punched cards using an electrical sensor. Following publicity about his invention, Hollerith established the Tabulating Machine Company which evolved into the International Business Machines Corporation, now commonly known as IBM.

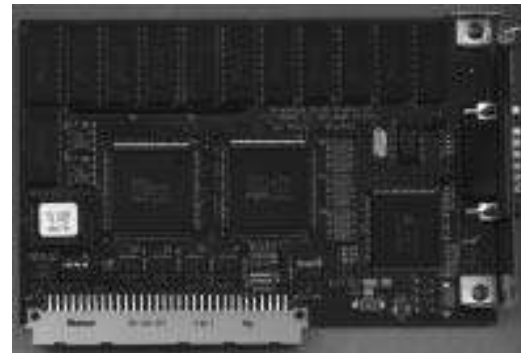
Computers have only been around since the middle of the 20th century, and personal computers didn't emerge until the mid-1970s, but the mechanisms for keystroke monitoring, and other aspects of worker surveillance have been in existence at least since the early part of the century.

Cyclometers were invented for counting keystrokes on typewriters, which provided a means to monitor the efficiency of clerical workers. Similarly, the work of telephone operators was monitored for decades. Operators were required to keep track of call statistics on cards they organized on their desks. Thus, the concept of monitoring both workers and client activities was already prevalent before computers were invented. So perhaps it shouldn't surprise us that computers were quickly adapted for surveillance purposes each time they evolved new capabilities.

Development of Electronics

Electronics were at the heart of the development of computers and a great deal of radio technology contributed to the evolution of the early computers. Vacuum tubes and printed circuit boards were two important technologies incorporated into computers and other electronic devices. The early history of vacuum tubes started with the *Fleming valve* and the de Forest *Audion* were described in the Radio Surveillance chapter. Circuit board design emerged gradually through the 1920s and onward.

A great deal of design work related to computers occurred within the U.S. military forces, especially the Army, where it was needed for ballistics targeting tables and complex calculations related to navigation and aiming and firing advanced weapons. Since many electronics inventions arose out of these activities, the development of printed circuit boards has generally been assumed to have been developed in the 1940s. However, an investigation of radio fabrication shows that at least a few radios from the late 1920s already had printed circuit board fabrications, indicating that the practice was invented earlier, even if it did not become prevalent until the 1950s.



Left: An example of a 1928 circuit board that was discovered in a commercial cabinet radio by Jonathan Winter, the proprietor of the Bellingham Antique Radio Museum. The copper traces have been blasted onto the underside of the circuit, with connections to the upper side through basic nuts and bolts (the wire jumpers were later additions). During the 1940s, the U.S. Army developed photolithographic processes for creating circuit boards for use in electronics and later in computers. Right: A modern printed circuit board can support tiny traces and computer chips. [Classic Concepts photos ©1998, used with permission.]

The Early History of Practical Computers

In Germany, in the 1930s, a brilliant young engineer named Konrad Zuse (1910-1995) developed a general purpose calculating and computing machine in his parents' apartment. The *Zuse Z1* had a mechanical memory storage and was programmed by punching instructions onto film. Later, with help from Helmut Schreye, electronic relays and vacuum tubes were added. By 1942, Zuse was developing the Z4, which was demonstrated in April 1945.

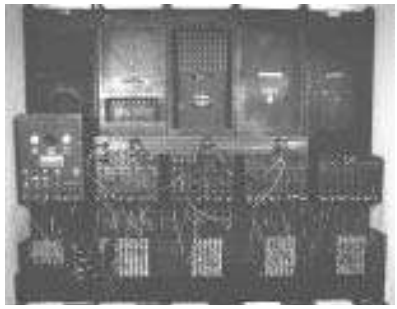
In Britain, the Colussus computer, involved in decyphering the German Enigma code, was being developed under complete secrecy during 1943. It became operational in 1944, a fact that wasn't publicly revealed for almost three decades later.

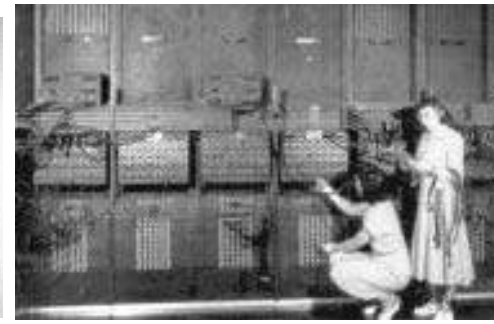
Meanwhile, in America, John Vincent Atanasoff (1903-1995) and Clifford E. Berry were collaborating on the development of the *Atanasoff-Berry computer* (ABC). It was prototyped in 1939 after two years of design development. It used rotating drum capacitors to refresh memory so that data wouldn't be lost. It is significant for the fact that the data and memory were implemented as separate functions. Data were entered into the computer with punch cards, a system that was still in use on many computers in the early 1980s.

Another computer developed in the late 1930s and early 1940s was the *Harvard Mark I*, an automatic relay computer constructed by Howard Aiken with support from IBM engineers. It could run long calculations from punched paper tape.

The *Electrical Numerical Integrator and Calculator,* better known as the ENIAC, was developed by John W. Mauchly and J. Presper Eckert at the University of Pennsylvania under the guidance of John Brainerd. The ENIAC was dedicated in 1943 and unveiled in 1946. When complete it weighed over 30 tons and included nearly 20,000 individual vacuum tubes.

Thus, the first gigantic, expensive, vacuum-tube computer systems were first introduced in the 1940s. They were little more than advanced calculating machines by current standards, costing millions of dollars, yet their capabilities far exceeded previous technologies. For the first two decades, because of their cost, they were used almost exclusively for large-scale government, science, and business uses. The average homeowner was barely aware of their existence until television shows began to feature computers and robots in the late 1950s and 1960s.

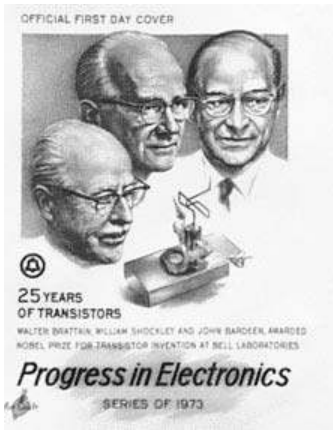


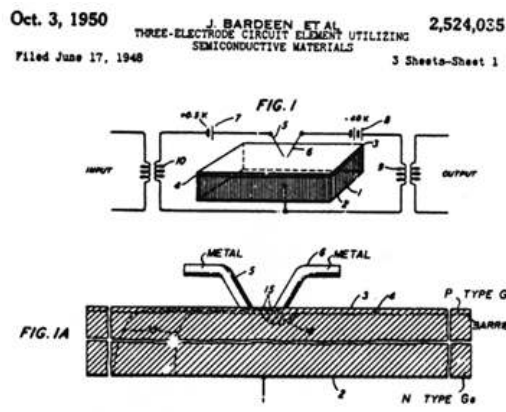


Left: The ENIAC computer, constructed in 1945 and rolled out in February 1946, was essentially a giant advanced calculator which was used for a variety of U.S. Army projects including ballistics calculations, scientific computing, weather prediction, and thermal ignition studies. Right: Programmers are shown changing the coding configuration by physically rearranging the wires. [U.S. Army historical photos, public domain.]

Grace Murray Hopper (1906-1992) was a mathematician, physicist, and pioneer computer scientist who developed the COBOL programming language in the days when computers were programmed by moving wires around. More important, however, was the fact that she realized that code could be reused, that routines could be self-referencing, even though many detractors scoffed at the idea at the time. But Hopper championed the basic concept, even though the technology was not yet in place, and her ideas established a foundation for other programming languages, which would come into their own when circuit boards and binary electronics superseded the old physically wired systems.

The early computers were limited in capabilities, difficult to maintain and program and yet, in spite of their limitations, they contributed fundamental calculations and tables that built a foundation for scientific advancement and future computing. Computers bootstrapped their own evolution by contributing to our understanding of physics and mathematics and to the development of electronics and more powerful computers.





Left: The inventors of the transistor were commemorated in this U.S. Postal Service first day cover. Right: A portion of the original patent for the transistor, which was registered by and subsequently granted to the inventors from Bell Laboratories. [Cover from the collection of the author, used with permission; U.S. Patent and Trademark Office, public domain.]

The invention of the transistor at the Bell Laboratories in 1947, following the end of the World War II, was one of the most significant developments in all of electronics history and had a big impact on the design of electronics from that point on. Not only could computers be made smaller and less expensive, but they could be made to perform functions that were not practical on the giant, tube-based systems. Compilers, assembly languages, and other aspects of programming continued to evolve, which, when combined with new systems, would herald in a new age of data processing and information exchange.

Innovative Ideas

When microcomputer electronics became a reality, many visionary thinkers were excited by the technology. Even though microcomputers didn't become established until the mid-1970s, a number of inventors had already envisioned a world of small computers by the 1960s. In 1968, Jürgen Dethloff proposed the idea of using a plastic card as the medium to support microelectronics, essentially describing a 'smart card' a decade before they became technologically practical. A few years later, Roland Moreno's idea of associating a personal identification number (PIN) with digital information led to the development of *magnetic stripe cards* that are now familiar transaction tools.

The Birth of Computer Networks

Computer networks, particularly the Internet, have had a profound effect on computer surveillance. There are several factors that brought about the birth of computer networks:

decreased size and price - As room-sized computers became smaller and less expensive, it became possible for organizations to own more than one. This facilitated experimentation and the evolution of networking hardware and software.

advanced calculating concepts - The idea of hooking computers together was seen as a way to collectively increase computing power over what a single machine or several individual machines could accomplish. If a computing task could be 'farmed out' to several computers and the data brought together through automation after the individual tasks were 'solved,' this could greatly speed up certain types of tasks. This idea of achieving more efficient *distributed computing* provided motivation for interconnecting computers.

time-sharing - As word about the improving capabilities of computers spread, more organizations were becoming interested in accessing computer services and were willing to pay for it. Time-sharing capabilities were developed so that individuals equipped with 'dumb terminals' could pay for computer time on large-scale systems. The idea of creating 'smart terminals' was not far behind. Network protocols were developed to facilitate dumb and smart terminal connectivity, eventually allowing multiple users to hook into a single system.

human social factors - The pervasive desire for people to intercommunicate was also a factor in the evolution of networking. The desire to send messages through computers motivated the invention of specific network communications tools such as email and newsgroups.

By the early 1970s, the ARPANET, the precursor to the Internet, was being developed by the U.S. Defense Advanced Research Projects Agency (DARPA). Modems that allowed computers to communicate through phone lines were being developed and improved at about the same time.

Microcomputer Electronics

When microcomputers as we know them were invented in the early 1970s, no one paid much attention. The Kenbak-1 rose and sank in 1971 with barely a whisper. It wasn't until the *Altair* was developed in 1974 and advertised and featured as a hobbyist kit in the January 1975 issue of Popular Electronics that the world suddenly took notice. Within two years, CRT screens and keyboards were standard peripherals and the Apple and TRS-80 lines of computers were launched. Microcomputers would soon become a tool of daily life.

Not long after microcomputers were introduced, hardware developers began selling modem cards that could be inserted in a microcomputer to allow it to interface with a phone line to share data with systems. These early modems were slow, only 300 bits per second, but that didn't deter hobbyists from using them. *Bulletin board systems* (BBSs), in which individuals could dial up a computer that was being used as a *server* for games and message boards became highly popular by the early 1980s and modem speeds increased to 1200 bits per second.

During the 1970s, Gary Kildall (1942-1994) developed CP/M, the first significant widely distributed microcomputer operating system. Other operating systems joined CP/M, including AppleDOS, TRS-DOS, and L-DOS, giving consumers a variety of options to use on their personal computers. The public eagerly began buying the new computers, paying almost $5,000 for a full system with some software, a modem, and a printer.* By the late 1970s, there was a fierce competitive battle between Apple, Radio Shack, and IBM to capture the microcomputer market.

A historic milestone in computing history occurred when Microsoft bought an operating system from a programmer named Tim Paterson, who had created a version of CP/M adapted from Kildall's CP/M manual. Microsoft sold this to IBM and it came to be known as PC-DOS. PC-DOS was then adapted by Microsoft as MS-DOS and sold in competition to IBM's operating system (much to IBM's surprise as they assumed they had purchased exclusive rights to the software). Kildall continued to develop CP/M which evolved into Digital Research's DOS (DR DOS). Thus, the competition for a major computer and a major operating system for home and business markets heated up and the microcomputer revolution was underway.

By the early 1980s, microcomputer sales were booming and computer networks were getting established. By the mid-1980s computers had found their way into many homes and schools. Since schools were particularly interested in networking connectivity, so that teachers could monitor student activities and students could work on group projects, Apple Computer built networking capabilities into their Macintosh computers right from the start. At the same time, Kildall's company was developing some of the first effective connectivity technologies for IBM-licensed technologies. On a bigger scale, DARPA was developing large-scale networks for military and scientific work. For home computers, dialup BBS systems were thriving, with thousands of users now sharing information and home-brew software through telephone networks. The speed of modems had now increased to 2400 bits per second.

By the mid-1980s FidoNet emerged as a way to automatically transfer files from one computer to another through phone lines. Thus, by 1984, networks were evolving rapidly on many fronts and eventually the technologies would converge into one system that came to be known as the *Internet.*

*In 1980, that was nearly the cost of a new car, a hefty price considering that computers operated only at 4 MHz and had only about 8 kilobytes (not Megabytes) of RAM. They stored information on tapes, not hard drives, and the monitors could only display 320 *x* 200 pixels.

Tiny Computers

As computer electronics devices dropped in size and price, developers continued to capitalize on the new technologies and seek ways to incorporate computing capabilities into new media. By the late 1980s, pen computers, schedulers, advanced programmable calculators, and smart cards began to emerge. In terms of surveillance, tiny computers provided a way to unobtrusively access data in the field and, when small radio modems emerged, to send that data to a central facility or individual colleague.

Magnetic stripe cards provided a way for the issuer of the card to track the movements and habits of the person using the card. Not all smart card issuers used them for this purpose, but the technology was in place and the possibility now presented itself. By the mid-1990s, retailers recognized the surveillance potential of 'member cards' and began offering discounts and other enticements to get customers to carry membership cards. It was now possible to track a person's shopping habits, including what types of products they typically purchased, how often they shopped, and how much they spent.

The 1990s - Increasing Integration and Processing Capabilities

The most significant advancements in computer surveillance in the 1990s, were profiling systems and computer-processed video systems.

Identity profiling

Profiling databases are systems that combine computer networks and magnetic stripe or other access devices to develop profiles on the attributes and actions of the people who use the technologies. These systems made it possible for supermarkets to profile shopping preferences and patterns and to target mailings and cash receipt advertising to the individual consumer. They allow financial institutions to profile client transactions and marketing professionals to use Web sites to profile potential customers. In many cases the customers have no knowledge or control over what is being done with the personal information that was being collected. Profiling is one of the areas over which privacy advocates have expressed special concern.

> ".... There exists a massive wealth of information in today's world, which is increasingly stored electronically. In fact, experts estimate that the average American is "profiled" in up to 150 commercial electronic databases. That means that there is a great deal of data–in some cases, very detailed and personal–out there and easily accessible courtesy of the Internet revolution. With the click of a button it is possible to examine all sorts of personal information, be it an address, a criminal record, a credit history, a shopping performance, or even a medical file...."
>
> [Mr. Kohl, speaking on a bill to establish the Privacy Protection Study Commission, in 1999.]

Audio/Video Integration with Computer Processing

Computer-processed video systems are video camera feeds that are analyzed by computer algorithms. These systems can identify faces, individuals, actions, movement, and a host of other triggers. By 2000, the systems were so sophisticated, they could even recognize people who were wearing hats, glasses, or beards. Some were integrated with audio sensors that could detect the sound of a traffic accident, aim a camera at the source of the sound, and record video images related to the accident.

In 1997, the American Management Association released survey statistics on midsize and large member companies, reporting that almost two-thirds were using some form of monitoring or surveillance. Worker productivity and accountability were cited as motivations for

monitoring. However, contradictory views were expressed by the U.S. Office of Technology Assessment, which reported that no reliable evidence yet supports the contention that monitoring increases production, but that stress does appear to increase.

In 1999, the American Management Association reported that 27% of large U.S. corporations check employee email on a routine basis.

These various reports indicate that surveillance is increasing, that it is becoming highly prevalent in the workplace, and that the types of devices used are also increasing in variety and sophistication. In the light of these changes, there have been many proposed bills and concerns about regulating use of the technologies.

5. Description and Functions

The three main areas of computer surveillance that have been introduced here have been surveillance of information on the Internet, computer profiling, and workplace surveillance. The technical aspects of computer surveillance including hacking, firewalls, proxies, and packet sniffing are outside the scope of this volume, but there are many excellent references on computer security that deal with these issues. Computer processing is also described here in a little more detail.

5.a. Internet Surveillance

A large proportion of the information that is surveilled on the Internet is *open source* information, which is information that is freely available. Web pages, chat rooms, and USENET newsgroups are all examples of open sources. Some of the major search engines were mentioned in the earlier part of this chapter. Additional useful sources of information include

discussion lists - unmoderated, moderated, or by-invitation discussion groups in which members participate in sharing information, data, and opinions. Discussion lists cover every conceivable topic and number in the tens of thousands. The best known public discussion lists are on USENET and are known as newsgroups. These are established on a vote process. Unfortunately, due to junk and advertising messages (which are not permitted), many newsgroups have gone to moderated status and some have simply died because the noise-to-signal ratio from irresponsible posters became too high. As a result a number of Web and email discussion lists have emerged to take the place of some of the better USENET groups of the past (there are still good computer newsgroups, but the general ones suffer from problems). Other sources of discussion lists include

http://www.liszt.com/

http://www.onelist.com/ which is now http://www.egroups.com/

yellow and white pages lists - free or commercial sources of 'phone book' style information on individuals and companies. Some also include email addresses. Some of the best known sites include

http://www.411.com/

http://www.411.ca/

http://www.infospace.com/

http://www.freeyellow.com/

http://www.whitepages.com/

http://www.yellowpages.com/

maps and travel locators - free or commercial sources of terrain and street maps (satellite images are discussed in the Aerial Surveillance chapter). Some of the popular sources include

http://www.mapquest.com/	city and street maps
http://www.maps.com/	world atlas, topographic maps
http://www.usgs.gov/	terrain and satellite maps

5.b. Computerized Profiling

Computerized *profiling* is the process of collecting data on a person's individual characteristics, personal information, or activities by monitoring their actions through voluntary reporting, access devices, or other surveillance technologies that can be interfaced with a database. It also applies to records kept on individuals convicted of criminal offenses, which include personal information, violations, fingerprints, and other data related to law enforcement.

The most common devices used for profiling include magnetic stripe cards (identity cards, ATM cards, supermarket or sports club membership cards, etc.) and video cameras. Other systems, such as biometric fingerprints and iris scans are now also being combined with computer databases.

Law enforcement, national security, and customs agencies use a wide variety of databases to profile visitors to the country, foreign agents, criminal suspects, convicted offenders, and prisoners. These databases are increasingly being linked together through the Internet to allow agencies to cooperate in cases that involve more than one state.

In the past, law enforcement agents working in patrol cars had to radio in driver's license information or license plates to ask the dispatcher if there were any outstanding warrants or other problems with a particular individual. New systems are now being put in place in which patrol officers can put the data directly into a mobile unit and call up any relevant data from a central database.

Joint automated booking stations (JABS) are multimedia information systems based on a DEA-Rome Laboratory pilot project to enable Federal law enforcement agencies to share information more effectively.

5.c. Work Monitoring Systems

The most prevalent forms of workplace monitoring using computer electronics include

- the use of access cards or keys that log an individual's entry and exit patterns and sometimes also their movements around a complex;
- the monitoring of keyboard input, use of computer applications, Internet activities, and email; and
- telephone activities, especially telemarketing calls, sales follow-up calls, and technical support calls.

"The range of occupations susceptible to electronic monitoring is surprisingly wide. Some of the positions most likely to be monitored include: word processors, data-entry clerks, telephone operators, customer service representatives, telemarketers, insurance claims clerks, mail clerks, supermarket cashiers, and bank proof clerks (OTA, 1987; ILO, 1993). Professional and technical workers may believe that their work is too com-

plex to be monitored successfully. However, sophisticated groupware applications and work-flow tracking systems provide an abundance of information on the status of an electronic document as it is "passed" from one professional to another. As well, electronic mail and scheduling applications provide additional potential for surveillance of employee activities and communications (Clement, 1988; ILO, 1993; Piller, 1993; Allen, 1994)."

[Susan Bryant, "Electronic Surveillance in the Workplace," Canadian Journal of Communication, V.20(4).]

5.d. Computer Processing

A technology that has been mentioned in a number of chapters is the capability of computers to manually or automatically analyze or clean up information from other surveillance devices. This is usually an expensive 'last resort' process, but in cases of murders or kidnappings, the technology can mean the difference between life or death for vulnerable victims. Two of the more common computer processing technologies include

data processing/exploitation - the process of enhancing an image or other data (e.g., sound) to clarify the source of the data or the identity of an object or person. For example, an image may be sharpened, or the colors or tonal values adjusted to make details more clear. Image processing can be used to clarify faint writing on a wall or a photo of a faint footprint in the mud. It can also be used to change the apparent age of a person in a photo, such as child lost for several years, or to remove or add a beard or glasses. It may further be used to clean up a poor audio signal taped from a phone call or to raise or lower the tone of a voice of someone who was using a voice changing device to hide his or her identity (e.g., a kidnapper).

data fusion - the process of combining data from more than one source. For example, video footage of a license plate may not show the numbers, but fusion of several frames of video, choosing the best parts of each frame and combining them, can sometimes yield a recognizable number.

The photo of the footprint on the left was difficult to see and no plaster cast was made of the print. In the photo in the middle, the image was processed with a common image processing software program to make the outline and ridges easier to identify and thus easier to match with its mate on the right. [Classic Concepts ©1999, used with permission.]

Computer processing is not limited to data we can see or hear. Patterns that are invisible to humans can sometimes be readily interpreted by special devices and computer processing. For example, infrared images called *thermograms* can be used to identify individuals. When

various types of data are combined and analyzed by the computer, it becomes almost impossible to hide your identity through disguises or changes in haircuts and facial hair.

Computer processing is not just used for examining evidence or identifying criminal suspects or unauthorized intruders, it may also be used in access systems for employees or those authorized to enter restricted areas.

6. Applications

This section does not constitute a complete list of all vendors, nor does it imply an endorsement of the quality of their products or services. The following are intended as educational examples only, to provide an introduction to the types of products that may be purchased on the market related to this topic.

Computer Spy Systems

Computer spy systems are products designed to monitor the various activities of a computer user, including keystrokes, password entries, applications, specific Web pages, Internet resources, and other files or data that are accessed or run. Some of these systems are intended to protect the security of a computer from unauthorized use, others are used to monitor workplace productivity or to collect evidence of unauthorized, incorrect or illegal use. Some are used to monitor the activities of children for parental or educational purposes. Occasionally they are used to steal or 'grab' passwords to allow someone to later access the system without authorization. Examples with a variety of purposes and capabilities include

Data-Trak, Inc. *WinSpy* - A Windows-based network surveillance software tool which allows a computer to monitor several others on a network. The software on the monitored systems will take screen captures of the desktop environment and send them in encrypted format to the WinSpy console which then displays the JPEG-format screen shots of the selected computers being monitored. The monitoring program is password-protected.

Codex Data Systems *DIRT* - Data Interception by Remote Transmission. A powerful surveillance tool sold only to authorized law enforcement and government agencies, this product is intended to aid users in reading encrypted messages. The system sends email to a target machine with embedded security software which will open up the system for covert access and monitor keystrokes to capture information and encryption keys which are subsequently transmitted to the sender when the target computer is online.

Omniquad *Detective* - This is a tool to retroactively construct the historical actions on the target computer system, including content downloaded from the Internet. System images can be viewed in a slideshow format. The software has advanced search capabilities.

MicroSpy (U.K.) *MicroSpy* - This consists of a microchip concealed in a short length of cable which is attached to the computer being investigated. It is designed to monitor keyboard characters and store them as they are typed, up to 1000 keystrokes. The device can be retrieved and can later be connected to the computer running the software and it will automatically upload the capture information (address, phone numbers, passwords). The device can then be reset and used again. Used in instances of embezzlement, tax evasion, computer fraud, and unauthorized access. U.K. patent pending. IBM-licensed compatibles.

Olivetti *Pandora* - A system for viewing remotely through video cameras associated with each Pandora station. The software includes Peek (employee approval) and Spy (no approval) modes.

Intrusion detection systems are based on the premise that people may try to access an unauthorized computer, access a computer that has been left unattended, or access programs or data without authorization. They detect an intrusion or anomalous use of a system, optionally log the activities on the computer, and optionally email or otherwise alert the owner or authorized user of the computer. They may also optionally shut down the system or prompt the user for authorization if anomalous activities are detected. They may even be programmed to turn on other detection devices such as video cameras or audio listening devices.

Ghost Keylogger - A computer security surveillance tool that monitors whether someone is accessing a secured computer. It can be used to monitor an off-limits computer or to monitor the computer activities of children. It records every keystroke to an optionally encrypted file which can be saved or sent to a specified email address. It further logs the title of the active application and the time of its use.

Tracking Systems

Tracking systems frequently combine radio or infrared transmitters with computer databases. There are now realtime programs that can plot the location of a person within the vicinity of the monitored premises and display the information on a picture of the premises on the computer monitor. Depending on the system, the computer can show the current location and recent path. These systems can be used for trucking and taxi services for safety, efficiency, and dispatch purposes. They can also be used to track workers in hazardous areas or visitors to a secured area. Similar systems are also used in some wildlife tracking programs.

Active Badge - A worn-badge system that contains an infrared transmitter which transmits a unique 48-bit word every fifteen seconds so that the location of the badge (and the person wearing it) can be tracked. Badge information in a database can include security clearance and personal information.

Video Peripherals

Computers are now commonly used to control, manage, and poll through inputs from video surveillance or biometric identity systems.

AITech *WaveWatcher-TV* - A hardware peripheral card for Windows-based IBM-licensed compatibles which allows realtime 21-bit full motion video to be displayed in a window within the Windows interface environment. It is positionable and sizable from full-screen to icon-size. It takes inputs from three independent NTSC or PAL video sources and three independent audio sources. It can be used with VCRs and closed-circuit television feeds for video conferencing and video surveillance. Individual frames can be captured, stored, and edited such that a VCR or camcorder can be used as a scanner.

Computer Database Systems

There are hundreds of database systems related to surveillance activities, including systems that hold mug shots, fingerprints, data on employees and contractors, and lists of sus-

pected foreign agents or terrorists. This is just a tiny selection of the many systems available:

Digital Justice Solution™ - by Printrak International Inc. This system combines realtime automated fingerprint identification, computerized criminal history, a mug shot, and document storage and retrieval capabilities. As of 1999, over 80 law enforcement agencies were linked to the system, with an average time of identification of about 15 minutes.

MADRID-LE™ - by Electronic Warfare Associates, Inc. This is a relational database system designed for law enforcement applications to support information analysis, storage, and retrieval of large volumes of investigative data from numerous databases.

TrueID™ - by Image Data, LLC. This is a means to enable a staff member to check the picture of a customer on file when he or she is making a transaction. First, picture ID is presented to the vendor, who inserts the photo into a scanner where it is transmitted and mapped into a customer database. Later, when a transaction takes place, the identity device can be queried on the customer and the image that is stored in the database is securely transmitted to the device and displayed on a small screen to the cashier or teller. The teller then verifies the image with the person seeking to make the transaction.

Other resources include the National Crime Information Center and the National Law Enforcement Telecommunications System. Many states have criminal history and sex offender databases, in addition to which there is a National Sex Offender database.

Government Alliances

In 1995, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and the Advanced Research Projects Agency (ARPA) signed a memorandum of agreement to cooperate in computer system security research and development. The Information Systems Security Research–Joint Technology Office (ISSR–JTO) was created to support these efforts and to aid in safeguarding data in Department of Defense (DoD) information systems.

7. Problems and Limitations

It is difficult to discuss problems associated with computer surveillance when the field is so diversified and still rapidly evolving. In most cases, the problems are social rather than technological. Technologists have made remarkable progress in solving individual problems, including increased storage capacity, speed, and connectivity. The rate of change still appears to be increasing and the capabilities of computers are far beyond what most people envisioned ten years ago.

The most prevalent problems appear to be associated with finding exactly what you want and managing the veritable flood of information that is currently available. Improved search algorithms, intelligent agents to located and filter information on the surveillant's behalf, and good prioritizing to separate the good information from the rest are probably the most important advancements that could be made to improve the efficiency of computer surveillance.

8. Restrictions and Regulations

Several regulations related to privacy in general have already been listed in the Chapter 1 and Chapter 2 and can be cross-referenced. Some that are more specific to computers in order of date include

Electronic Communications Privacy Act of 1986 (ECPA) - Updates the Crime Control Act of 1968 to protect digital communications from interception and disclosure. It requires a court order for Federal agents to conduct a 'wiretap' on electronic communications, including data, video, and audio, from unauthorized interception.

Computer Security Act of 1987 - Public Law 100-235. Sets standards for security and mandates for sensitive systems. The Act created the Computer System Security and Privacy Advisory Board (CSSPAB) as a public advisory committee. The Board was to identify security issues and provide advisement.

Computer Matching and Privacy Protection Act of 1988 - An amendment to the Privacy Act of 1974 that expressly regulates matching of data from different databases (federal, state, local). It requires notification of matches and provides an opportunity for the findings to be challenged. This has been further amended.

Telecommunications Infrastructure Act of 1993 - Prohibits telecommunications carriers from disclosing subscriber information of a personal nature.

Wiretapping

There are strict laws against the interception of electronic communications, as included in the *U.S. Wiretap Act*, and amended by the *Electronic Communications Privacy Act of 1986*. These are covered in some detail in the Audio Surveillance chapter. There are some exceptions for employers who, as providers of email systems, may retrieve stored messages, but only in the normal course of employment.

Workplace Monitoring

With the increase of computer monitoring and logging of employee activities, sometimes down to individual keystrokes, there has been concern by labor organizations about protection of employee rights within an increasingly surveillant work world. One example of this is the consideration and publication of a report on *Telecommunications and Privacy in Labour Relationships* by the *European Union Data Protection Commissioners* released in 1996. The paper discusses various data-collection methods used in the workplace and their potential to generate data on employee activities. The second part includes a number of recommendations for the respect of privacy in the workplace. The third part includes specific applications of the report recommendations to information technologies and telecommunications. At about the same time, the *International Labour Organisation* was also discussing a draft Code of Practice with regard to privacy. These developments indicate the trend toward assessing workplace policies in the light of new technologies.

9. Implications of Use

Workplace Surveillance with Computers

There are a number of problems associated with computer surveillance and assessment of workplace performance. Computers tend to be used to surveil activities that are easy to quantify. Since management activities are less quantifiable than production line work or data entry activities, there is a stronger focus on monitoring the activities of workers with less senior-

ity or authority, establishing a double-standard in the workplace beyond what already exists. All people make mistakes. If an employee who is not surveilled makes a mistake, there is often no record of the event and an opportunity for the individual to remedy the mistake. In computer surveillance systems, every mistake, every hesitation, every learning step can be recorded with chilling accuracy, making it possible to create 'justifications' for layoffs, firings, or blocked promotions or raises which affect only certain workers and which may be unfair in the broader context of the workplace.

> "Today 40 million American workers are under surveillance at the office. Women make up 85 percent of that number, as they tend to occupy customer-service and data-entry positions, which are more commonly scrutinized."
>
> [Brad Marlowe, "You Are Being Watched," *ZDNet,* Dec. 1999.]

While Marlowe is correct in pointing out the preponderance of surveillance in traditional office jobs staffed by women, men are not exempt from workplace surveillance. Truck drivers, cab drivers, travelling sales representatives, and many production line workers are male and are also likely to come under heavier surveillance as the technologies become easier to install and monitor.

Computer surveillance has the potential to caused increased stratification in society, separating the 'workers' from the executives more than in the past by one-way monitoring that provides data to the executive that are not available to the worker. This dichotomy of documentation would become especially apparent in legal suits. Courtroom judgments are based largely on concrete evidence. If there is a dispute between an employer and an employee, the employer has the opportunity to gather reams of 'substantive data' on an employee through computer surveillance, in the form of computer logs and video tapes, while the employee may have little or no substantive proof to prosecute or defend against actions of an employer.

In some cases, employers are justifiably concerned about employee abuse of computing facilities. If employees use workplace computing systems to make purchases of illegal goods or are downloading illegal images and the actions are traced to the employer's premises, there may be a problem defending the actions and determining who, in fact, was responsible for the illegal actions. This, in part, has motivated employers to put workplace surveillance in place. In some states, employers must inform employees before using surveillance tools, but this is not universally required at the present time.

Balancing Costs and Losses

Computerized surveillance is changing the workplace. Rather than being structured on trust and communication among employees and managers, offices are increasingly being equipped with video cameras, electronic access and tracking technologies, and computer activity logs. This 'automation' does not come free. Not only can it be expensive to install and maintain all the equipment, but it can be unprofitable to constantly monitor, archive, and search and retrieve the enormous volumes of data that can be recorded. Employers have to weigh the losses traceable to a small percentage of dishonest employees against the cost of buying, maintaining, and monitoring workplace surveillance equipment. They must further assess the impact on productivity that may occur if employees feel they are being controlled by intimidation rather than being motivated by trust.

Data Mining and Personal Privacy

The use of computer networks for data mining creates a problem for individuals who are unaware of the extensive amount of information that can be collected about them and dis-

seminated without their knowledge. It is difficult or impossible to have your name removed from many of the lists on the Internet. Some of the more reputable directory sites allow you to log on and 'unlist' your number, but as soon as they update their data from newly released phone directories, about once a year, your name is usually back and you have to do it again. Less reputable directory sites sell your information and may not provide a way to have your name removed. Even if you remove it, it may already have been replicated by a hundred computers around the world and then the information is 'out there' and impossible to recall. If you don't have a computer and network account to spot the exploitation in the first place, you're out of luck.

Powerful Programs in the Wrong Hands

There are a number of software programs that have been developed for law enforcement officials and government agents to capture information, files, and keystrokes on target machines. Many of the companies selling these products are careful to qualify the buyers so the software doesn't get into the wrong hands. However, not all companies are so discriminating in distributing software and piracy of software is rampant on the Internet.

If software algorithms designed for covert law enforcement agents were to get into the hands of criminals, it would give them the tools to examine the contents of millions of computer systems. How do users know that the technology is not being used by the suppliers themselves to make covert examinations of networked computers? Law enforcement agents have to operate under certain legal restraints related to wiretapping and often require authorizations to use this type of tool. However, unauthorized users of the software accept no such similar constraints. There are currently few laws to protect the public from this type of spying, because they rarely know their systems have been violated.

Computers Integrated with Video Systems

Many computer cams have been integrated with the Web so that Internet users anywhere can log onto a Web site and remotely control the swivel-and-zoom cameras to watch any aspect of the scene that they choose. This is wonderful for schools, zoos, and museums who want to give shut-ins, children, and other Internet patrons a chance to see the animals, educational materials, sports events, cultural events, and exhibits, but what about the cams that are mounted on campuses and downtown buildings? Could a stalker use the cameras to chart the movements of a coed walking home from classes at the same time every day? Could a corporate spy use them to monitor the customers walking into or out of a store each day?

Public Sales of 'Private' Information

As was mentioned in earlier sections, a number of Public Safety Departments have sold or attempted to sell driver's license photos to outside private agencies without public input or approval. In some cases, the public found out and had the deals stopped but in one case, at least, the judge ruled that driver's license photos are not protected by privacy laws (e.g., South Carolina). Since there is a precedence now for government agencies to exploit public information, does this open the door for these agencies to sell other kinds of information kept in databases? (Note that the *Driver's Privacy Protection Act of 1997* regulates how records may be released and how the recipients of records may subsequently distribute the information.)

10. Resources

10.a. Organizations

No endorsement of these companies is intended nor implied and, conversely, their inclusion does not imply their endorsement of the contents of this document.

American Management Association International (AMAI) - This development and training organization considers matters of employee testing and monitoring and periodically issues the results of surveys, including surveys on Electronic Monitoring and Surveillance. http://www.amanet.org/

Computer Emergency Response Team (CERT) - Established in 1988 by the Defense Advanced Research Projects Agency (DARPA) to respond to security problems in networked computers and computer networks, particularly the Internet. CERT supplies technical assistance to aid in protecting the digital infrastructure. http://www.cert.org/

Computer Operations, Audit, and Security Technology (COAST) - This is now part of CERIAS. It is a cooperative project, multiple-lab computer security research established at the Computer Sciences Department at Purdue University. http://www.cerias.purdue.edu/coast/coast.html

Computer Security Institute (CSI) - Since 1974, CSI has been dedicated to serving and training computer security professionals. http://www.gocsi.com/

High Tech Crime Investigation Association (HTCIA) - An international association which promotes education, research, and discussion about the investigation of high technology crime. http://www.htcia.org/

National Computer Security Association (NCSA) - Security assurance services for Internet-connected companies. ICSA publishes Information Security Magazine. http://www.icsa.net/

National Computer Security Center (NCSC) - Originally established by the Department of Defense (DoD) for certifying various computer systems for security.

10.b. Print

Bentham, Jeremy, "The Works of Jeremy Bentham," New York: Russell & Russell, 1962.

Casey, Eoghan, "Digital Evidence and Computer Crime," Academic Press, 2000, 279 pages. Presents technical and legal concepts discussing the application of computer forensics.

Chantico Publications, "Combating Computer Crime: Prevention, Detection, Investigation," New York: McGraw-Hill, 1992.

Conly, Catherine H., "Organizing for Computer Crime Investigation and Prosecution," Washington, D. C.: U.S. Dept. of Justice, 1989, 124 pages.

Icove, David, "Computer Crime: A Crimefighter's Handbook," O'Reilly & Associates, 1995.

Ilgun, Koral, "USTAT - A Real-time Intrusion Detection System for UNIX," Master's Thesis, November 1922, U. C. Santa Barbara.

Judson, Karen, "Computer Crime: Phreaks, Spies, and Salami Slicers," Enslow, 1994.

Power, Richard, "Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare," San Francisco: Computer Security Institute, 1995.

Rule, James B., "Private Lives and Public Surveillance: Social Control in the Computer Age," New York: Schocken Books, 1974, 382 pages.

Stephenson, Peter, "Investigating Computer-Related Crime," Boca Raton, Fl.: CRC Press LLC, 2000.

Zuboff, Shoshana, "In the Age of the Smart Machine: The Future of Work and Power," New York: Basic Books, 1988.

Articles

Aeillo, John R., "Computer-Based Work Monitoring: Electronic Surveillance and its Effects," *Journal of Applied Social Psychology,* V.23, pages 499-507.

American Management Association International (AMAI), "More U.S. Firms Checking E-Mail, Computers Files, and Phone Calls," 14 April 1999. A report on an annual survey of 1,054 member organizations conducted from Jan. to Mar. 1999. Reports on the prevalent and increasing trend of electronic workplace monitoring.

Attewell, Paul, "Big Brother and the Sweatshop: Computer Surveillance in the Automated Office," *Sociological Theory,* V.5, pages 87-99.

Balitis, John J., Jr.; Silvyn, Jeffrey S., "Big Brother at Work: Supervision: Employers' electronic monitoring of employees in the workplace raises federal and state liability issues," *Daily Journal*, April 1998.

Boehmer, Robert G., "Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop," *DePaul Law Review*, V.41, pages 739-819.

Bryant, Susan, "Electronic Surveillance in the Workplace," *Canadian Journal of Communication,* Papers, V.20(4). Describes increasing prevalence of monitoring and of power of the corporation over the individual worker along with legislative and public policy concerns.

Burgess, John, "'Active Badges' Play Follow the Worker: Computerized Trackers Spark Worries about 'Big Brother,'" *The Washington Post*, 8 October 1992.

Bylinsky, Gene, "How Companies Spy on Employees," *Fortune*, 1991, V.124, pages 131-140.

Denning, Dorothy E., "An Intrusion Detection Model," *IEEE Transactions on Software Engineering,* Feb. 1987, Number 2, p. 222.

DeTienne, Dristen Bell; Nelson, T. Abbot, "Developing an Employee-Centered Electronic Monitoring System," *Journal of Systems Management,* 1993, V.44, pages 12-16.

"The End of Privacy: The surveillance society," Editorial, *The Economist,* 5 Jan. 1999.

Gandy, Oscar H., Jr., "The Surveillance Society: Information Technology and Bureaucratic Social Control," *Journal of Communications,* 1989 V.39, pages 61-76.

Griffith, Terri L., "Teaching Big Brother to be a Team Player: Computer Monitoring and Quality," *Academy of Management Executive,* 1993, V.7, pages 73-80.

Iadipaolo, Donna Marie, "Monster or Monitor? Have Tracking Systems Gone Mad?" *Insurance & Technology,* 1992, V.17, pages 47-54.

Jewett, Christina, "Your Life: Private as a Postcard," *Indiana Daily*, 13 Oct. 1999.

Levy, Michael, "Electronic Monitoring in the Workplace: Power Through the Panopticon," Impact of New Technologies Web Server, *Library and Information Studies,* UC Berkeley, 1993. The author looks at the impact of workplace monitoring with quotes from a number of significant writings on the subject at the time.

Lunt, Teresa F., "A survey of intrusion detection techniques," *Computers and Security,* 1993, V.12, pp. 405-416.

Marlowe, Brad, "You Are Being Watched," *ZDNet,* Dec. 1999. Workplace monitoring.

Marx, Gary T., "Let's Eavesdrop on Managers," *Computerworld*, 20 April 1992, p. 29.

National Security Agency, "Information Security and Privacy in Network Environments," *Office of Technology Assessment OTA-TCT-606,* U.S. Government Printing Office, Sept. 1994.

Nitzberg, Sam, "Emerging security issues involving the presence of microphones and video cameras in the computing environment," *ACM SIGSAC Security Audit & Control Review,* 1996, V.14 (3), pp. 13-16.

Nussbaum, Karen, "Workers Under Surveillance," *Computerworld*, 6 January 1992, p. 21.

Piller, Charles, "Bosses with X-Ray Eyes," *MacWorld*, 10 July 1993, pages 118-123.

Rome Laboratory Law Enforcement Technology Team, "Transferring Defense Technology to Law Enforcement," *The New Horizon,* April 1996.

Schwartau, Winn, "DIRT Bugs Strike," *Network World*, July 1998. Describes the Data Interception by Remote Transmission system which is sold only to authorized government and law enforcement personnel.

Sundaram, Aurobindo, "An Introduction to Intrusion Detection," *Crossroads.*

Vitone, Philip, "Reflections on Surveillance," *Canadian Journal of Communication,* V.19(1).

Journals

Note, the U.S. Navy has a very good list of computer communications-related journals at http://chacs.nrl.navy.mil/ieee/cipher/readers-guide/journals.html

"Canadian Journal of Communication," includes articles on privacy and computer surveillance. http://www.cjc-online.ca/

"Cipher," a newsletter of the IEEE Computer Society's TC on Security and Privacy.

"Computer Underground Digest," a weekly electronic journal available without a subscription fee. It can be found on the Web and at *comp.society.cu-digest.*

"Crossroads," an electronic publication of the ACM that discusses various computer-related topics. http://www.acm.org/crossroads/

"Information Security Magazine," published by ICSA for Internet-connected security assurance services professionals.

"Journal of Computer Security," quarterly journal of research and developments.

"Law Enforcement & Corrections Technology News Summary," a publication of the National Law Enforcement and Corrections Technology Center of the National Institute of Justice.

"The Risks Digest," Forum on Risks to the Public in Computers and Related Systems, sponsored by the ACM Committee on Computers and Public Policy.

10.c. Conferences and Workshops

Many of these conferences are annual events that are held at approximately the same time each year, so even if the conference listings are outdated, they can still help you determine the frequency and sometimes the time of year of upcoming events. It is very common for international conferences to be held in a different city each year, so contact the organizers for current locations.

Many of these organizations describe the upcoming conferences on the Web and may also archive conference proceedings for purchase or free download.

The following conferences are organized according to the calendar month in which they are usually held.

"NDSS '01," The Internet Society network and distributed system security symposium, San Diego, Ca., 7-9 Feb. 2001.

"NetSec," network security technical conference, San Francisco, Ca., 12-14 June 2000.

"Safecomp 2000," Rotterdam, The Netherlands, 24-27 Oct. 2000.

"ICICS 2001," 3rd international conference on information and communications security, Xian, China, 13-16 November 2001.

"International Conference of Data Protection Commissioners," 13th conference in 1999.

"National Computer Security Conference," jointly organized by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for attendees from private industry and the government.

10.d. Online Sites

The following are interesting Web sites relevant to this chapter. The author has tried to limit the listings to links that are stable and likely to remain so for a while. However, since Web sites do sometimes change, keywords in the descriptions below can help you relocate them with a search engine. Sites are moved more often than they are deleted.

Another suggestion, if the site has disappeared, is to go to the upper level of the domain name. Sometimes the site manager has simply changed the name of the file of interest. For example, if you cannot locate http://www.goodsite.com/science/uv.html *try going to* http://www.goodsite.com/science/ *or* http://www.goodsite.com/ *to see if there is a new link to the page. It could be that the filename* uv.html *was changed to* ultraviolet.html*, for example.*

Electronic Monitoring & Surveillance. A survey published online by the American Management Association International. This site includes charts, tables, discussion, and a summary of key findings. When viewing this site keep in mind that there was a large upswing in the installation of video cameras in 1999 that may change the demographics somewhat from those published in this 1997 survey. http://www.amanet.org/survey/elec97.htm

Note: If you don't enjoy typing in long Web addresses (URLs), you can access the links on the support site set up by the author for your convenience. http://www.abiogenesis.com/surveil

10.e. Media Resources

"Criminals in Cyberspace," an *Arts & Entertainment* program from the 20th Century with Mike Wallace series. It provides a look into cybercrime and the types of terrorist activities that can occur on computer systems. VHS, 50 minutes. May not be shipped outside the U.S. and Canada.

"Cybersex Cop," an *Arts & Entertainment* program from the Investigative Reports series which discusses pornography and the impact of pornography on the Internet, including the arrest of a child pornographer. VHS, 50 minutes. May not be shipped outside the U.S. and Canada.

11. Glossary

Titles, product names, organizations, and specific military designations are capitalized; common generic and colloquial terms and phrases are not.

CCH	computerized criminal history
EPM	electronic performance monitoring
firewall	a computer security configuration intended to selectively or completely limit access to a system or process
gateway	a transmission connection between dissimilar networks which may or may not have security features incorporated into the system
IDS	intrusion detection system
packet sniffer	a technical tool for analyzing and monitoring the data packets that are transmitted over a computer network
proxy	a system or software agent intended to act on behalf of clients and which can act as a server or client for processes associated with security