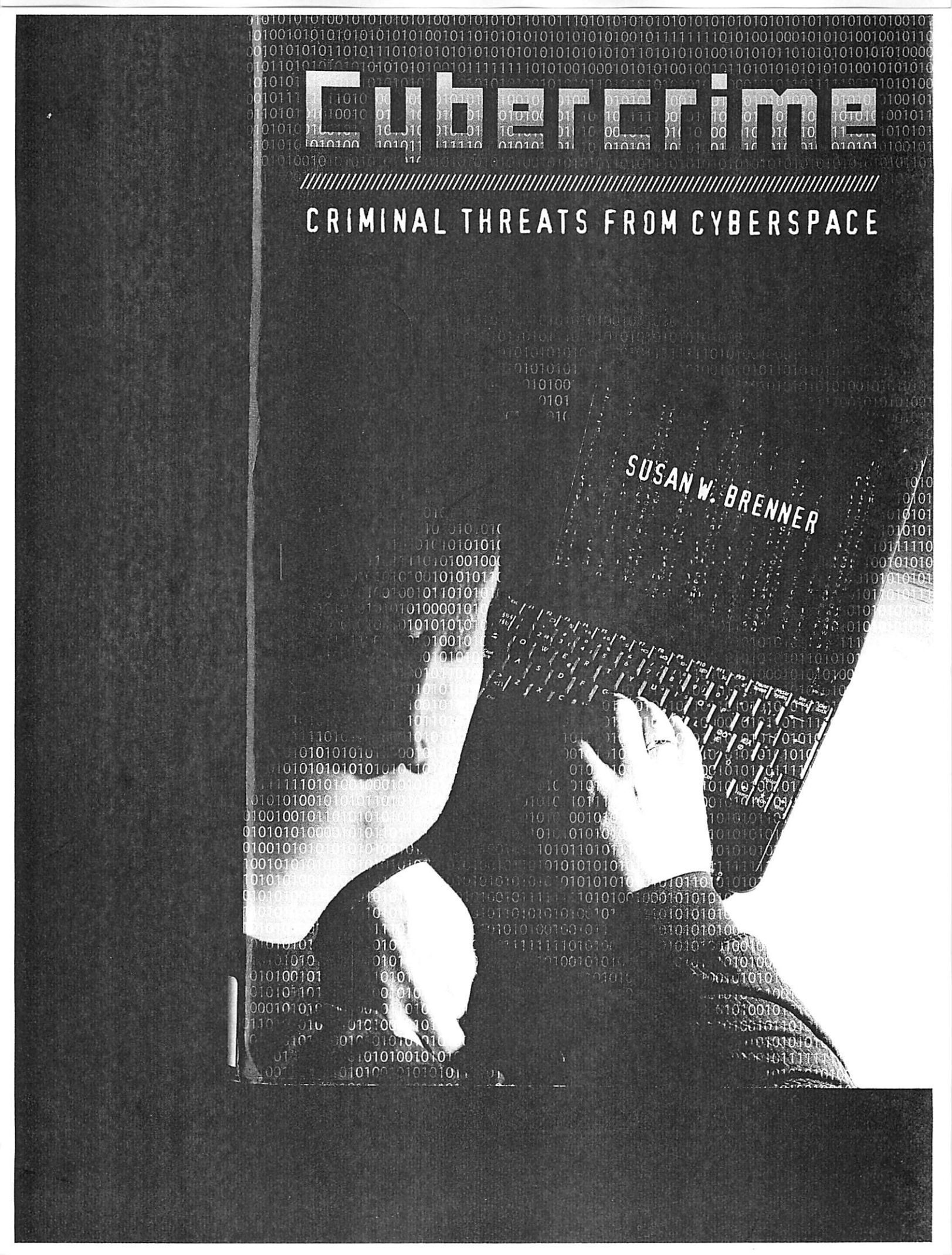
Cybercrime

CRIMINAL THREATS FROM CYBERSPACE



As we saw in Chapter 2, hacking is a kind of trespass. Trespass has been a crime for centuries, probably for millennia. Definitions of the crime are straightforward, as this Colorado criminal trespass statute illustrates: "A person commits . . . criminal trespass if such person unlawfully enters or remains in or upon premises of another."[3] Real-world criminal trespass statutes are designed to protect the privacy and sanctity of real property (i.e., land and structures built on land) by discouraging people from going where they have no legal right to be.

As we saw in Chapter 2, hacking is analogous to trespassing, in that hackers gain access to computers without being authorized to do so. Because computers are a kind of property (personal property, instead of real property),[4] hacking is similar to trespassing on someone's land. Therefore, we could have expanded criminal trespassing statutes so they outlawed hacking as well as trespasses on real property,[5] instead of creating a new "hacking" crime. The problem with trying to adapt traditional, criminal trespassing laws to encompass hacking is that one type deals with conduct in the physical world while the other deals with conduct "in" the virtual world. As we will see in Chapter 4, that difference undermines the viability of analogizing hacking and trespass. Trespassers physically "go into" a place or "go onto" land; hackers neither "go into" nor "go onto" the computers they attack. The evil to be outlawed in hacking laws is not unauthorized physical presence in a "place"; it is, as we will see in Chapter 4, something far more complex and elusive.

Disseminating malware can also be analogized to a traditional real-world crime: vandalism. Vandalism laws make it a crime to intentionally damage or destroy "real or personal property of another" without the owner's consent.[6] As we saw in Chapter 2, viruses and worms can damage computer systems and/or destroy data, both of which qualify as personal property. So we could expand our definition of vandalism, which currently focuses on inflicting physical damage to property, to also encompass the damage and destruction caused by viruses, worms, and other types of malware. No U.S. jurisdiction seems to have taken that approach, presumably because of the conceptual and practical differences between physical damage and intangible damage to property.

If someone takes a sledgehammer to my laptop, that would clearly be vandalism; my laptop, my personal property, has been damaged (or, more likely, destroyed). If that same someone creates and spreads a virus that infects my computer and deletes data, that could reasonably be characterized as vandalism; the virus has destroyed personal property (the data). If that virus infects my laptop, but instead of deleting data, it interferes with the operating system on which my computer relies to function,[7] it is not at all clear that this would constitute vandalism. The laptop itself has neither been destroyed nor damaged; it is still capable of functioning. The software constituting the operating system has not been deleted (destroyed) nor has it been damaged, at least not in the traditional sense; it is presumably still capable of functioning once the virus has been neutralized. In this and similar malware scenarios, the "harm" inflicted is at once more subtle and more complex than the "harm" encompassed by vandalism statutes.

Unlike the physical damage inflicted on tangible personal property in vandalism cases, the "harm" inflicted on the laptop in this scenario can be remediated, and the laptop can be restored to its original condition with comparatively little effort. Compare this scenario to one in which someone throws paint or acid on Rembrandt's *The Night Watch*.[8] If the vandal threw paint, it *might* be possible to restore the painting to a state only somewhat degraded from its original condition. If the vandal threw acid, it will be impossible to restore the painting to any semblance of its original condition. As I hope this hypothetical case demonstrates, the ultimate difference between real-world vandalism and the dissemination of malware lies in the elasticity and malleability of digital property. The "harm" I sustain in my original scenario is more akin to interference—or nuisance—than it is to the "harm" inflicted by vandalism.[9] For that and other reasons, the law has not sought to bring malware within the definition of vandalism. Instead, as we will see in Chapter 4, it created new and distinct malware crimes.

There is one other target crime we need to consider before we take up the tool cybercrimes: Distributed Denial of Service (DDoS) attacks. In a DDoS attack, attackers overwhelm Web sites and servers by bombarding them with data, or "traffic." The effect of a DDoS attack is similar to what would happen if someone used an automated dialing system to repeatedly call a small pizza delivery business; the automated calls would tie up the phone lines of the business and prevent legitimate customers from placing orders. The consequence would be that the business would lose business at least for as long as the attack continued. It might also lose some residual business if customers decided not to try calling again, either on that occasion or in the future.

In a DDoS attack, the perpetrators use a network of compromised computers—known as "zombies"—to send massive bursts of data at the target (s) of the attack. The zombies are computers that have been taken over by "bots"—software that subtly and usually invisibly infiltrates a computer. Bot software turns innocent computers—those used by individuals, businesses, and governmental, educational, or other agencies—into zombie computers.[10] The owners of these compromised computers usually have no idea their equipment is now moonlighting as a minion of some more-or-less

sinister force.[11] The computer will operate more or less normally. The user may notice that it is running a little slower than usual, but that may be the only indication it has become a zombie.

Zombie computers will be integrated into a network—a "botnet"—controlled by a cybercriminal known as the "botherder." Botnets are becoming huge; law enforcement officers report botnets consisting of two million zombies, and the size only increases. A botnet is, in effect, a digital zombie army. Botherders usually rent their digital armies to cybercriminals, who use them to make money by shutting down Web sites and extorting money from their owners, sending spam e-mails, enticing users into online fraud scams, or installing adware on users' machines.

A botnet-based DDoS attack does not fit into the definition of any of the crimes countries have traditionally recognized. A pure DDoS attack is not theft, fraud, extortion, vandalism, trespass, or any other heretofore known type of criminal activity. DDoS attacks require the adoption of new laws, which we will examine in Chapter 4.

TOOL CYBERCRIMES

Instead of being the target of a cybercrime, a computer can be the implement—the tool—that is used to commit it. For the cybercrimes in this category, the role of the computer is analogous to the role telephones play in telephone fraud.[12]

Fraud is a type of theft. As a court noted, one commits theft when he or she takes personal property owned by someone else and carries it away "with intent to steal the property."[13] Theft consists of taking someone's property without his or her permission and with the intent to permanently deprive the victim of the possession and use of that property. Fraud is a relatively new variation of theft. The crime of fraud was created to encompass the situation in which the victim willingly gives the property to the criminal—the fraudster. If the owner of property consensually gives that property to someone, intending that the person will keep it, this is not theft; it must be something else. Centuries ago, English common law developed the crime of fraud, which consists of persuading someone to give you their property under false pretenses, such as falsely telling a person that in exchange for the property, you will give that person title to the Brooklyn Bridge. Fraud is also known as theft by trick.

Until the twentieth century, fraud could be committed only by mail or in person. In the twentieth century, fraudsters began using the telephone to commit fraud because it allowed the fraudster to remain anonymous and

speed up the process. A perpetrator could contact people more quickly by using the telephone than he could in person. The telephone became a tool that is used to commit fraud; in the same way, and for many of the same reasons, computers have become a tool that is used to commit fraud and a variety of other crimes.

Perhaps the best example of a tool cybercrime is the Citibank theft case. In August 1994, Carlos Arario, head trader at the Argentinian firm Invest Capital, came to work one morning and discovered that more than $200,000 had disappeared overnight from his firm's account with Citibank.[14] Four anonymous wire transfers were made from the Invest Capital account to four unknown accounts. Arario called Citibank executives in New York to tell them what had happened; unfortunately, it continued to happen, and over the next months, someone siphoned almost $10 million from 20 Citibank accounts.

Citibank executives assembled a "war room" of experts to try to stop what was happening, but they could only watch as funds were transferred from client accounts into accounts in California, Tel Aviv, Rotterdam, Athens, Latin America, Finland, and Israel. The experts launched a global investigation as they sought to track the transfers and prevent more from occurring. They got a break when the unknown cyberthief transferred $218,000 from an Indonesian businessman's account to a BankAmerica account in San Francisco. Citibank experts and federal agents traced the account to Evgeni and Erina Korolkov, Russian nationals who had come to the United States from St. Petersburg. Erina was arrested when she tried to make a withdrawal from the San Francisco account. (She and Evgeni had allegedly opened this and other accounts to launder the funds being stolen from Citibank.) Federal agents flew to St. Petersburg and were given access to records that showed the Citibank accounts were being accessed from a computer at AO Saturn, a software company in St. Petersburg.

By December, Erina was cooperating with federal authorities and encouraged her husband to help them identify the Citibank thief. After the FBI promised Evgeni they would treat him leniently if he cooperated, he identified Vladimir Levin, who worked at AO Saturn, as the cyberthief. Levin was then a 29-year-old computer programmer who allegedly used a laptop computer at the AO Saturn offices to carry out the Citibank fund transfers. As these agents were identifying Levin, other federal agents were arresting Russian mules in the Netherlands and other countries The mules' role was to collect the funds that had been transferred from Citibank accounts to foreign accounts. Citibank ultimately claimed it had recovered all but $400,000 of the stolen funds.

Because the United States and Russia did not have an extradition treaty, Levin was safe as long as he remained in Russia. For some reason, he flew to London in 1995, where British authorities arrested him. He spent 18 months in a British jail, fighting extradition. Levin was finally sent to the United States and indicted on federal charges of theft and hacking. In 1998, he pled guilty and was sentenced to three years in prison.

Many do not believe Levin was the sole architect of the Citibank thefts (or almost thefts). Many found it difficult to believe Levin, even working with associates, could have developed and implemented the complex international network of bank accounts and mules that was to have been used to launder the proceeds. Many also did not believe Levin had the computer skills necessary to hack the Citibank accounts. Various theories emerged to explain what "really" happened. According to one theory, a Russian hacker group known as Megazoid figured out how to access the Citibank computers. One of them sold that information to Levin—or to someone working with Levin —for $100 and two bottles of vodka.[15] As to how Levin implemented the network of international bank accounts and mules, some, including then-U.S. Attorney General Janet Reno, suggested Levin was directly or indirectly working for the Russian mafia, which was, and still is, involved with cybercriminals.[16]

We will probably never know exactly what happened with the Citibank crimes: whether Citibank did, indeed, recover most of the money; whether Levin acted alone in hacking the Citibank system and transferring the funds from the Citibank accounts; and whether the Russian mafia was involved, either at the outset or as a broker for the stolen funds. At the time, Citibank confessed that its experts had never quite figured out how the crimes—or frustrated crimes—were executed. All of that, though, is irrelevant to the point at hand. Whoever he or she was, the architect of the Citibank thefts was a post-twentieth-century bank robber. Instead of using a mask and a gun to steal from a bank, the thief used computers. He or she used a new tool to commit a very old crime.

As we will see in Chapter 5, theft is only one of a host of traditional crimes that can be committed by substituting computer technology for more conventional means. Tool cybercrimes also include fraud, embezzlement, stalking, forgery, threats, extortion, defamation, gambling, terrorism, homicide, and the dissemination of child pornography. None of the tool crimes is a "new" crime, but it may be difficult to prosecute tool crimes under existing law, an issue we will take up in Chapter 5.

COMPUTER INCIDENTAL

The third and final category consists of cybercrimes in which the use of a computer is incidental to the commission of the crime; the computer plays a minor role in the offense. This category encompasses cases in which a computer is used to commit a crime; however, its use is so trivial that the computer does not rise to the level of being a tool, the use of which is integral to the commission of the crime. To understand the difference, it is helpful to consider an example.

Armed robbery is a type of theft. As we have already seen, theft is taking someone's personal property without his or her permission and with the intent to permanently deprive him or her of its possession and use. Theft requires only that the thief take the property without the owner's consent. It is theft if I take your laptop while you are not looking. I took it without your consent, but I did not use force to take it. Robbery consists of using force to commit theft. A Colorado statute, for example, defines robbery as taking "anything of value from . . . another by the use of force."[17] The force can consist of inflicting "bodily injury" on the victim or threatening to inflict such injury. The most serious theft crime is armed robbery, which, as its name implies, consists of using a deadly weapon (usually a gun) to commit robbery. Armed robbery is considered the most serious theft offense because the use of such a weapon increases the risk that someone will be killed in the commission of the offense. Armed robbery cannot be committed without using a deadly weapon; such a weapon is the tool the robber uses to commit this particular crime and, as such, is an integral element of the offense.

Computers were essential to the commission of the thefts in the Citibank case; Vladimir Levin, or whoever committed these crimes, could not have siphoned funds from the Citibank accounts without using computers (and the Internet). Computers played an integral role in the commission of these crimes; they were the tool the use of which was essential for the crimes to have been committed as they were. Now, that does not mean we need to define a new crime—computer theft—to encompass what Levin and others have done. We define armed robbery as a distinct type of robbery because the use of a deadly weapon—another tool for committing theft—raises distinct concerns about the "harm" inflicted in these crimes. As we will see in Chapter 5, while the use of computers to commit theft enables the crime be committed in new ways, it does not increase the actual or potential "harm" inflicted in a way that requires us to define a new crime. We can simply treat the computer as one of many tools that can be used to commit theft.

Now consider a different scenario: In 2007, Melanie McGuire was convicted of killing her husband William. According to prosecutors, Ms. McGuire used chloral hydrate to sedate William and then shot him "three or four times" before dismembering his body and dumping the remains in the Chesapeake Bay.[18] After the remains were discovered, police began investigating the crime. They learned Ms. McGuire had purchased a gun of the type used to kill her husband shortly before the murder; the murder weapon was never found. Police computer forensic investigators examined the couple's home computer and found that in the weeks before the murder, someone—presumably Melanie McGuire—used the computer to research topics such as "how to commit murder," "how to illegally purchase guns," and "undetectable poisons." They also found "romantic e-mails" between Melanie and her boss, a married physician. At trial, prosecutors used the computer evidence to establish that Melanie had a motive for killing her husband (i.e., to be with her lover) and had researched methods of committing homicide, including methods that were used in her husband's murder. On April 23, 2007, Melanie was convicted of murder; on July 19, she was sentenced to life in prison for the crime.

The McGuire computer played an important, although peripheral, role in William's murder. Melanie used it to research how to commit the crime but not to commit it. As we will see in Chapter 5, computer technology can—and no doubt will—be used to kill human beings. Here, however, the McGuires's home computer played an incidental role in the commission of the offense; it facilitated the commission only in the most indirect sense. Its actual role—as is true whenever a computer plays an incidental role in the commission of a crime—was as a source of evidence. The police clearly suspected Melanie of killing her husband, but the evidence preserved on the computer made their case much stronger than it would have been otherwise.

The McGuire case illustrates the role the computer plays in this final category of cybercrime. As people increasingly use computers, computers are increasingly used in criminal activity. It is, for example, common for drug dealers—especially those who deal on a large scale—to use computers to track their drug purchases, inventory, and sales.[19] As in the McGuire case, these computers become a valuable source of evidence when a drug dealer has been apprehended and will go on trial. The same is true for a variety of crimes: white-collar crimes such as embezzlement and economic espionage; other murders; blackmail; extortion; and essentially any crime we can imagine. We will examine this aspect of cybercrime in detail in Chapter 5.

Because the computer is merely a source of evidence in these types of cases, they do not require us to adopt new legislation to be able to prosecute the crimes at issue. But as we will see in Chapter 6, the intricacies of digital evidence can make it necessary to revise laws that govern the acquisition of evidence and its introduction at trial.

7

Beyond *War Games*: Who Are the Cybercriminals?

This chapter deals with an issue we have been covering throughout this book: the people who commit cybercrimes. In many of the previous chapters, we focused on the cybercriminals of years past, the teenaged hacker of *War Games* being the prime example.

In this chapter, we will examine what are, in effect, cybercriminal archetypes. That is, we will examine the kinds of people who commit three types of cybercrime: two target crimes (hacking and insider attacks) and two tool crimes (fraud and stalking). We focus on these crimes because they tend to be the most frequently committed types of cybercrime. The frequency with which these crimes are committed makes it possible to generalize with some accuracy about the people who are most likely to commit them.

HACKERS

For many people, hacking is the archetypal cybercrime, and the *War Games*-style hacker is the archetypal cybercriminal. That is not an unreasonable conception of cybercrime and cybercriminals. As we saw in Chapter 2, cybercrime really began with hacking, and the first hackers were sport hackers—students who saw hacking as an intellectual exercise. The original hackers hacked for fun, not for profit.

As we saw in Chapter 2 and succeeding chapters, that model of hacking is in decline, if it has not disappeared entirely. We still have occasional sport hackers, but today, even adolescents tend to hack for instrumental reasons (i.e., because they are seeking some benefit or advantage). In 2008, for example, Omar Khan, a high-school student in Orange County, California, was charged with 69 felonies under state law, based on his allegedly having hacked the computer system in his high school.[1] Among other things, Khan was accused of hacking into the system and changing test scores and grades. News stories speculated that he made the alterations to improve his chances of being admitted to a prestigious college.

David Lightman, the hero of *War Games*, also hacked his school's computer to change grades for himself and his friend;[2] for him, that was an aberration. Similar to his real-life counterparts, Lightman's primary interest was exploring computer technology, but he was not above exploiting it for personal advantage on occasion. By the beginning of the twenty-first century, that dynamic seemed to have reversed itself. News stories about adolescents who used their computer skills to explore systems had been replaced by stories about teenagers who, in similar ways to those of Khan, used their computer skills to exploit systems for personal advantage.

The reversal of that dynamic is not a sign that American adolescents are more unprincipled than they used to be. It is a function of the fact that computer technology is vastly more advanced than it was a quarter of a century ago. In the *War Games* era and for more than a decade afterward, computer technology was functionally analogous to automobile technology in the early part of the twentieth century. Those who owned cars back then had to know more than how to drive one. They had to know how to maintain a vehicle and how to fix it on the frequent occasions when it broke down.[3] The same was true for personal computer users in the 1980s and early 1990s. The operating systems in use at the time required a level of hands-on expertise and tinkering that was analogous to the mechanical expertise that was a basic survival skill for early car owners.[4]

At the beginning of the twenty-first century, the computer-automobile technology analogy is still valid but for different reasons. Modern vehicles are so reliable and so sophisticated that their owners no longer need mechanical expertise; all we do is drive. The same is true for twenty-first century computer technology: The operating systems that have been in use for roughly a decade are so self-contained and so sophisticated that we do not need the expertise that was *de rigueur* until relatively recently. Similar to modern car owners, all we do is use the technology.

That may account for the decline, if not the disappearance, of sport hackers. The generations that are growing up with modern computer technology are accustomed to using computers to do things instead of using them to learn how computers operate. Another factor that no doubt contributes to the decline in sport hacking is the Internet. As we saw in earlier chapters, the original hackers spent a great deal of time gaining access to networks and figuring out what they could do with them once they got access. Today, networked access is a given. Instead of having to use their computer skills to access a network, our David Lightmans use their skills and the Internet to do other things, such as changing grades, perpetrating hoaxes, and even committing cybercrimes.[5]

As we will see in Chapter 8, when law enforcement officers deal with cybercrime, they often confront an issue that historically seldom arose with crime: perpetrators who are in a foreign country. That issue frequently arises when law enforcement officers deal with the professional hackers who use their computer skills to commit the cybercrimes we surveyed in Chapters 4 and 5. Some professional hackers operate from inside the country whose citizens they victimize (e.g., from inside the United States). Many, though, do not. Conversely, although most of the declining pool of sport hackers are residents of the country whose systems they attack, some are not. We will return to the issues transborder cybercrime raises in Chapter 8.

INSIDERS

As we saw in Chapter 2, hacking began with insiders because they were the only ones who could exploit mainframe technology for improper purposes. In Chapter 4, we saw how that kind of insider hacking evolved into the current crime of exceeding one's authorized access to a computer or computer system. In Chapter 4, we reviewed some insider hacking cases, all of which involved more or less disgruntled employees.

Insider attacks have become a serious threat to computer security. The U.S. Secret Service conducted two studies of the insider threat. One focused on the banking and finance industry, and the other examined critical infrastructure sectors.[6] The researchers defined insiders as "individuals who were, or . . . had been, authorized to use the information systems they eventually employed to perpetrate harm."[7] They found that while there were similarities among the insiders within each group, there were notable differences between the banking and finance insiders and the insiders who worked in critical infrastructure sector positions.

The banking and finance industry study found that attacks "were not technically sophisticated or complex. . . . [T]hey typically involved exploitation of non-technical vulnerabilities such as business rules or organization policies . . . and were carried out by individuals who had little or no technical expertise."[8] Most attacks were planned in advance and were committed out of a desire for "financial gain, rather than a desire to harm the company."[9] A few were revenge for being fired.[10] Surprisingly, the attackers did not share a common profile. Most did not hold technical positions, did not have a history of launching technical attacks, and were not perceived as problem employees.[11] They ranged from 18 to 59 years old, and 42 percent were women.[12] Many of them were considered excellent employees. A man who "committed credit card fraud after 10 years of outstanding service in the banking field" was "well-paid and well-respected as a top salesman for the territory he managed."[13] Ultimately, this study concluded that the insider threat in the finance industry is a particularly complex phenomenon because it involves "an interaction among organizational culture, business practices, policies, and technology, as well as the insiders' motivations and external influences."[14]

The findings in the complex infrastructure sector study differed in several respects from those in the finance industry study.[15] For one thing, 86 percent of the insiders worked in technical positions: systems administrators (38%), programmers (21%), engineers (14%), and information technology specialists (14%).[16] Most (77%) were or had been full-time employees of the organization they attacked; 8 percent were or had been consultants and 8 percent were or had been temporary workers.[17] Age was again irrelevant; the critical infrastructure insiders were from 17 to 60 years old and were racially and ethnically diverse.[18] Ninety-six percent of them were males.[19] The most striking difference between these insiders and the banking and finance insiders was in the motives for the attack: 84 percent of critical infrastructure insiders were motivated "at least in part by a desire to seek revenge."[20] Ninety-two percent of the attacks were triggered by a "specific event or series of events" that included "employment termination (47%), dispute with a current or former employer (20%), and . . . demotion or transfer (13%)."[21] Similar to the banking and finance insiders, these insiders planned their attacks in advance. However, unlike the banking and finance insiders, most (80%) of the critical infrastructure insiders had been cited for "tardiness, truancy, arguments with coworkers, and poor job performance."[22]

The critical infrastructure insiders seem to have done more damage: "Eighty-one percent of the organizations experienced a negative financial impact as a result of the insiders' activities. The losses ranged from a reported low of $500 to a reported high of 'tens of millions of dollars.' "[23] Twenty-six percent of the organizations also suffered a "negative impact to their reputations."[24] Among other things, these insiders

- severed communication with affected organizations due to networks, routers, servers, or dial-up access being shut down;
- blocked sales due to blocked sales applications or deleted sales records;
- blocked customer contact due to modified customer passwords;
- damaged or destroyed critical information assets, such as proprietary software, data, computing systems, and storage media necessary to the organization's ability to contract work, produce product, or develop new products;
- damaged supervisory integrity, including exposed personal or private communications embarrassing to a supervisor.[25]

Because the vast majority of critical infrastructure insider attacks were triggered by a desire to seek revenge for a work-related event, these researchers concluded that the most effective way to address this type of attack is for organizations to implement policies that address "negative employment-related events."[26]

Although the Secret Service studies may seem too narrowly focused to allow us to generalize about those who launch inside attacks, the banking, finance, and critical infrastructure organizations involved in the studies actually represent a wide range of activities.[27] More importantly, they examined the two basic types of inside attacker: financial workers motivated by greed; and aggrieved employees who, unlike aggrieved employees in the past, have the skills and tools they need to revenge themselves on the employers whom they believe have treated them unfairly.

What the financial insiders are doing is not new. Insiders have been embezzling funds from financial institutions for centuries. Computer technology may make it easier for someone to embezzle funds or conceal the embezzlement, but neither the conduct nor the crime that results from the conduct is something we have not dealt with in the past. Financial insider attacks replicate history in another respect: Banks historically refused to prosecute embezzlers for fear the public would lose confidence in an institution if they learned it was susceptible to embezzlement.[28] They usually fired the embezzler and ignored the crime. The same thing happens with financial insider attacks. Banks and other financial institutions often do not report their crimes to law enforcement, preferring to dismiss them and avoid embarrassing publicity.[29]

What the other insiders are doing is new in one respect: the amount of damage the insider can cause. In the past, disgruntled employees stole office supplies, padded their expense reports, and took similar measures to exact revenge on the companies they believed had treated them unfairly. Today, every large organization necessarily hosts a cadre of insiders who can, if they so desire, cause tremendous damage to the company. Businesses and other organizations therefore are facing a serious new problem. While the insiders' motives are not new, the tools available to them are new. Because the tools an aggrieved employee can use to harm his employer tend to be the same tools he uses in his work, it is very difficult, if not impossible, to prevent attacks by dedicated insiders.

Because insiders, by definition, attack computer systems owned by their employers, they usually reside in the country where the systems they attack are located. That may change as offshoring and other trends increase the frequency with which people who live in one country are employed by a business or organization that is either physically or nominally "located" in another country.

FRAUDSTERS[30]

As we saw in Chapter 5, fraud is one of several financially motivated crimes that have migrated online. As we also saw in Chapter 5, those who commit online fraud can be in the United States but often operate from abroad.

As we will see in Chapter 8, cyberspace gives criminals the ability to target victims who are halfway around the world. This not only increases the pool of available victims, it also makes it easier for the online perpetrators to avoid being identified and apprehended by law enforcement. We will take up the law enforcement implications of transnational cybercrime in Chapter 8. Our focus here is on the people who commit cybercrimes, especially fraud.

In March 2009, the computer security company Finjan issued a report on its investigation of an online fraud operation based in the Ukraine.[31] The Ukrainian fraudsters implemented a scheme that was simple and ingenious: They hired rogue technical experts to inject specific, carefully chosen keywords into hundreds of legitimate news and shopping Web sites. Some of the keywords were misspellings of popular search terms, such as "Obbama" instead of "Obama." Others were "trendy keywords taken from the Google Trends system."[32]

Once seeded into a Web site, the keywords were picked up and indexed by search engines such as Google, which meant the search engines sent people to

the altered Web sites. When someone's browser took him or her to one of the altered Web sites, scripts the experts had embedded into the altered Web pages sent him or her to an external site that sold fake antivirus software. When the victim arrived at that site, a barrage of pop-up messages appeared, warning that his computer was infected with viruses and other malware. The messages told the victims they needed the antivirus software being sold on the site to eliminate the infection. The antivirus software, of course, was worthless; it could not have removed any malware that might have been on a purchaser's computer.

The Finjan researchers surreptitiously monitored the scam for 16 days. During that period, more than 1.8 million people were redirected to the fake antivirus site, and 7–12 percent of them bought the fake software, which sold for $20 to $50.[33] According to the Finjan report, if these returns were extrapolated " '[b]ased on a normal work week, this would put [the operators of the scam] in the $2 million-plus annual income bracket'."[34] It also noted that the experts the operators of the scam hired to alter legitimate sites and drive traffic to the fraud site were paid "about $10,800 . . . a day for their work."[35]

Although this may seem an isolated instance of cyber-fraud, it in fact exemplifies the basic online fraud dynamic.[36] What we see today is a twenty-first-century version of the nineteenth-century snake oil peddlers who sold fake remedies in the Old West. A snake oil peddler rolled into a town, set up shop, put on a great show for potential customers, sold his worthless product to as many people as possible, and then left town before the victims could figure out they had been had.[37]

Online scams such as the one described above transpose that dynamic into a new context. Instead of going to a town to find potential victims, the fraudsters trick the victims into coming to a Web site they control. Similar to a snake oil peddler, the fraudsters make sure that the Web site puts on a great show, whether it is pitching software or drugs or some other product. Similar to their historical counterpart, online fraudsters sell their bogus product or service to as many victims as possible and then close up shop and disappear to make it as difficult as possible for law enforcement to find them, on the off chance that law enforcement might try to find them.[38]

The impetus for all of this is the Willie Sutton principle we examined in earlier chapters: the premise that criminals will "go where the money is." Today, the money is increasingly online for several reasons. One is that we are spending more time online and conducting more of our activities online. As we become used to shopping, investing, and banking online, we become more confident in our ability to handle the online world and

correspondingly less hesitant about trusting certain Web sites or opportunities.[39] A second reason, I believe, is that many of us implicitly assume that what happens online is not "real" and therefore cannot harm us. People who might never trust a stranger who walked up to them on the street and offered them a chance to make millions by helping him smuggle money out of Morocco do exactly this when the stranger contacts them online.

Finally, there is another, even more important reason why the Willie Sutton effect is so pronounced in cyberspace: Fraudsters can go where the money is in a way they could not when we lived our lives exclusively in physical space. A century ago, it would have been functionally impossible for someone in the Ukraine to defraud people in the United States, England, France, and all the other countries whose citizens fell prey to the fake antivirus software scam. There were mail fraud scams 100 and more years ago, but they inevitably tended to target people in the same country, if not in the same general area. What that meant is that U.S. citizens had to worry about being defrauded only by other U.S. citizens (unless they traveled abroad and fell prey to a foreign scam artist). Cyberspace changes that; it gives aspiring scam artists in any country the ability to target victims in wealthy countries such as the United States and United Kingdom.

It is only logical that given a choice between a victim who has little money and a victim who has (or is perceived to have) a lot of money, a fraudster will target the latter. Those who were responsible for the Ukraine antivirus scam presumably live in Eastern Europe, which is the point of origin for a great deal of the world's cybercrime. It is also an area in which jobs tend to be scarce and wages low, both of which exacerbate the Willie Sutton effect. If a talented hacker has a choice between working as a low-paid but honest furniture mover or becoming a wealthy online fraudster, he may choose the dark path, especially if, as we will see in the next chapter, he runs little risk of being caught and prosecuted for his crimes. The consequences of that choice, which is being made all over the globe, create and shape much of the cybercrime we see today.

STALKERS

Unlike fraudsters (who are consistently motivated by greed), online stalkers are driven by various motives. Those who study stalking have developed taxonomies in an effort to parse out what drives those who in effect persecute other. Because stalking emerged as a real-world crime,[40] many of the taxonomies tend to focus on conduct that takes place in physical space, such as following the victim or damaging his or her car or other tangible property.

I have, though, found a taxonomy I think captures the motives that are common to online stalkers, such as those we examined in Chapter 5. This taxonomy divides stalkers into four categories: ex-partner stalking, infatuation stalking, delusional fixation stalking, and sadistic stalking.[41]

The creators of the taxonomy believe ex-partner stalking is the most common of the four categories of stalking. They note that this type of stalking is likely to involve the use of threats and that the stalker's motivations derive from issues of power, control, and freedom.[42] The Joelle Ligon case was an extreme instance of ex-partner cyberstalking.[43] An ex-boyfriend used the Internet to torment Ligon for six years. Among other things, he posed as Ligon in chat rooms, where he solicited men for sex and gave them her phone numbers. In an effort to get away from him, Ligon moved from Virginia to Seattle, but he followed her. He e-mailed her Seattle co-workers, claiming to be a representative of a group that enforced honor codes for colleges, including Ligon's alma mater. The e-mails claimed Ligon got her college degree under false pretenses and had a history of sexual deviance and drug use (none of which was true). After trying unsuccessfully to interest state prosecutors in the case, Ligon finally convinced federal prosecutors to charge her stalker with online harassment.

That brings us to the second category in the taxonomy. The taxonomy's authors believe infatuation stalking occurs less often than ex-partner stalking but is far from uncommon.[44] In this type of stalking, the victim is not the target of the stalker's anger and resentment but is the focus of a romantic fantasy. The stalker obsessively pursues the object of his or her desire, often sending him or her small gifts or messages. The stalker may also obsess about knowing where the victim is and what he or she is doing at any particular time. According to the creators of the taxonomy, infatuation stalkers are not likely to be dangerous and/or to threaten their victims, either overtly or implicitly.

The only reported case I can find that seemed to involve infatuation stalking is a civil case. In this case, a female student became a professor's research assistant. According to the civil complaint the student ultimately filed, the professor became increasingly infatuated with her over the semester, "telling her routinely that he loved her and asking questions about her . . . sex life."[45] When she resigned as his research assistant, he sent her an e-mail that said, "'Don't marry someone you can live with, Marry someone you can't live without.'"[46] After university authorities declined to discipline the professor, she filed a sexual harassment suit against him. I cannot find what the outcome of the suit was, although I suspect it was settled. Although I have not been able to find other reported cases dealing with similar conduct,[47] I

suspect this kind of stalking is quite common, especially online. I think we hear little about it because, as the creators of the taxonomy noted, infatuation stalkers are more of an annoyance than a threat. As a result, their victims are probably able to deal with the problem themselves, instead of having to go to the authorities for help.

Stalkers who fall into the third category, on the other hand, can be dangerous. In delusional fixation stalking, the stalker is so fixated on the victim that he or she believes they are in a relationship when, in fact, they may never have met.[48] This type of stalking often involves a status imbalance between the stalker and the victim. The victim often has some type of elevated or noteworthy status, such as a professor or other professional, a local or national celebrity, or a local person who is not famous but is held in high esteem in the community. This type of stalking is often characterized by "the incessant bombarding of the" victim with phone calls, e-mails, and other communications.[49]

A story from the United Kingdom illustrates delusional fixation stalking. Alexis Bowater, a "TV newsreader" for a British broadcasting company, was "bombarded . . . with abusive and sexual emails" from a 24-year-old man she had never met.[50] Over a period of two years, the anonymous stalker repeatedly sent his pregnant victim e-mails that were threatening and of "'an extremely explicit sexual nature.'" Police were finally able to identify the man, and he eventually pled guilty to charges arising from the stalking. In another case from the United Kingdom, a 42-year-old student at a university fixated on one of her professors, sending him so many e-mails he had to "close down the account because it became clogged."[51] The professor finally got a restraining order against her, but she ignored it. His stalker was finally convicted of violating the restraining order.

These two cases illustrate not only the dynamic that defines delusional fixation stalking but another aspect of it as well. The authors of the taxonomy divide delusional fixation stalking into two types: dangerous and less dangerous.[52] The 24-year-old who stalked the newsreader fell into the first category; the 42-year-old who stalked the professor fell into the second category. Both exhibited the core characteristics of this type of stalking (i.e., fixation on the victim, assuming a relationship that did not exist, bombarding the victim with unwanted communications), but the tenor of the messages each sent was quite different. The newsreader received e-mails that alternated between threats to harm her and her baby and graphic sexual fantasies. The e-mails the professor received contained "confused ramblings and often included inappropriate suggestions." The content of the first stalker's communications reasonably caused his victim to fear for her safety and that of her unborn child. The content of the other stalker's communications aggravated and infuriated her victim but apparently did not cause him to fear either for his safety or for the safety of his family. Although these cases arose in the United Kingdom, anecdotal evidence indicates that both types of delusional fixation stalking occur in the United States and in other countries as well.

All of this brings us to the fourth and perhaps most disturbing category in the stalking taxonomy: sadistic stalking.[53] The authors of the taxonomy note that this type of stalking often begins with an initial "low-level acquaintance" between the stalker and the victim that ultimately escalates until the stalker seeks to exert control "over *all* aspects . . . of the victim's life."[54] They explain that the sadistic element of this type of stalking lies in the stalker's desire to obtain "evidence of the victim's powerlessness" in order to validate his feeling of being in control.[55] The victim becomes the "obsessive target" of the stalker and usually has no idea why he has targeted her. This type of stalker is likely to expand the scope of his activities to include the victim's "family and friends . . . in a bid to isolate the victim and further enhance" his feeling of control.[56] The communications the stalker sends to the victim tend to be a "blend of loving and threatening" content, the purpose of which is to "destabilize and confuse" the victim.[57]

The best example of sadistic cyberstalking I know is a case that arose in Los Angeles in 1998.[58] Gary Dellapenta, a 50-year-old security guard from North Hollywood, tried to develop a romantic relationship with a woman from his church, but she made it clear she was not interested. Some time afterward, she began receiving calls and visits from strange men who told her they were ready to fulfill her fantasy of being raped. In all, six men showed up at her home, all with the same purpose. Some arrived when she was there but left when she said there had been a mistake. When she spoke to two of the men on the phone, she learned why they thought she wanted them to rape her: They had been in an online chat room with someone who used the victim's name and address. The person who posed as this woman in the chat room sent messages to the men, telling them "she" fantasized about being raped and inviting them to fulfill her fantasy. "She" gave them the woman's home address and phone number and even the security code to her alarm system.

When the victim realized what was happening, she recruited her father, who went online to find out where the messages were being posted. He found them in chat rooms hosted on two sites that offered users anonymity. The father began participating in the chat rooms and soon found himself corresponding with the person who was pretending to be his daughter. As with the other men, the person sent to the woman's father her home address,

phone number, and the code to disable her alarm system. At that point, the father and daughter went to the police, who were able to identify Dellapenta as the person who assumed the daughter's identity in the chat rooms. Officers searched the home he shared with his mother, seized Dellapenta's computer, and found the evidence they needed to charge him with cyberstalking. Dellapenta eventually pled guilty to the charge and was sentenced to serve six years in prison for what he had done.[59]

Although the technology Dellapenta used to target his victim was primitive compared to what we have today, the psychological tactics he used and the motives that drove him perfectly illustrate sadistic stalking. We can only imagine the terror his victim felt when men bent on rape began showing up at her home or calling her. We understand why that was happening, but she did not, at least not while it was happening. We can imagine the sadistic delight Dellapenta must have taken in his power to manipulate his victim, to destroy any sense of security she had in what should have been her haven—her home.

SUM

As this survey of selected cybercrimes illustrates, computer technology makes it possible to commit traditional crimes (e.g., theft, fraud, extortion, defamation) online. At the moment, most cybercrime consists of traditional crimes being committed in nontraditional ways because most cybercrime is, as we saw in earlier chapters, financially motivated. For financial crimes, the cybercriminal's motive and the harm he inflicts are essentially indistinguishable from the motives and harms inflicted by his real-world counterparts. All that differs is the methodology used by the perpetrator in committing the crime.

As this survey of cybercrime also illustrates, however, there is a residuum of cybercrime that differs markedly from the crimes we so far have seen being committed in the real, physical world. Dellapenta's cyberstalking is an example: In the real world, he could never have posed as his female victim, at least not with the credibility he enjoyed online. The cyberworld gave Dellapenta the ability to inflict new and devastating harm on his victim because he was able to turn the victim's "self" against her; that is, he was able to make it appear that what was happening to her was something she, herself, had orchestrated. The power to do that—to assume and exploit someone else's identity—may have existed in some minimal form prior to the Internet, but cyberspace magnifies that power and makes it available to anyone with a basic set of computer skills and a skewed mind-set.

These and other cybercrimes are the result of a phenomenon we examined in earlier chapters: Cyberspace empowers criminals in new ways—ways that, as we will see in the next three chapters, make it difficult for law enforcement to react effectively to cybercrime.

efforts to encourage countries to adopt consistent cybercrime laws will resolve these problems. I do not. We will return to this issue in Chapter 12, where we examine the viability of this and other proposals for improving the enforcement of cybercrime law.

First, we need to consider a related issue: the inherent tension between policing and individual privacy. We take up that topic in the next chapter.

11

Privacy versus Security: Which Trumps?

INTRODUCTION

There is an inherent tension between policing and privacy. As we saw in the last chapter, police are charged with investigating crimes that have already been committed, identifying the perpetrator(s), and apprehending him, her, or them. As we also saw, an effective law enforcement reaction to completed crimes is essential to discourage enough people from committing crimes that a society is able to maintain the level of internal order it needs to survive and prosper. The need for an effective law enforcement reaction also encompasses a related task: preventing crimes from being committed. Police also work to identify crimes that are in the planning and preparation stages so they can interrupt the would-be criminals before those criminals can inflict actual harm on someone or something.[1]

Both of these tasks are based on the police's ability to collect information about crimes that have been committed and crimes that will be committed. As a society, we want our police to collect information and solve or prevent as many crimes as possible. However, we also want them to stay within certain limits as they collect this information. We do not want the police to be able to violate individual privacy, at least not unless they comply with certain legal requirements. These requirements are intended to resolve the tension between policing and privacy by allowing the police obtain information

when they can demonstrate a compelling need for it and by preventing the police from intruding into our privacy when they cannot demonstrate such a need.

This chapter examines the requirements U.S. law imposes on police in their efforts to collect the evidence of a crime. As we will see, these requirements come into play only when the police's investigatory efforts intrude or threaten to intrude on an area or an activity that is legally defined as "private." Our law, similar to that of other countries, is not concerned with regulating police conduct that is designed to obtain information that is public or is in a public area.

The United States is a very large, very complex nation-state. It encompasses a substantial geographical area and has a population of more than 300 million people.[2] It is also organizationally complex. As we saw in Chapter 9, the United States has a number of federal police agencies and more than 17,000 state and local police agencies. Because the United States is a federal system, there are federal laws plus a distinct set of laws for each of the 50 states plus the District of Columbia and five U.S. territories.[3]

If the laws adopted by each of the states and territories could trump the laws of the federal government and the laws of the other states and territories, the United States would descend into a state of legal cacophony. It would be nothing more than a loose confederation of independent sovereign states. As we saw in Chapter 9, that describes the United States under the Articles of Confederation, but the Constitution changed that.

Article VI of the Constitution declares that

> [t]his constitution and the laws of the United States which shall be made in pursuance thereof . . . shall be the supreme law of the land; and the judges in every state shall be bound thereby, any thing in the constitution or laws of any state to the contrary notwithstanding.[4]

The Constitution also makes it clear that the federal government is to respect the states and the laws they adopt. The Tenth Amendment says the "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States." And Article IV of the Constitution says that each state is to give "full faith and credit" to the "public acts, records and judicial proceedings of every other state."[5]

Therefore, states can adopt their own laws as long as those laws do not infringe on the powers reserved for the federal government. Likewise, the federal government can adopt laws as long as those laws do not infringe on powers reserved to the states. This system has certain consequences for laws

that define the privacy of U.S. citizens: As long as those laws are implementing provisions of the U.S. Constitution, including the amendments that have been added to it, they are valid because the constitution is the "supreme law of the land." This is true regardless of whether the laws in question are adopted by the federal government or by a state.

The federal government can adopt only those laws that are authorized either by the explicit language of the Constitution or by powers the Constitution delegates to the federal government. On the other hand, the states can adopt laws that go beyond the provisions of the Constitution, as long as they do not conflict with those provisions or are otherwise illegal. For example, a state could not adopt a law reestablishing slavery because the Thirteenth Amendment to the Constitution abolished slavery "within the United States or any place subject to" its jurisdiction. However, states can adopt laws that legalize gay marriage because marriage is not a matter the Constitution delegates to the federal government; therefore, marriage is an issue reserved for state law under the Tenth Amendment.[6]

That brings us back to privacy: The Constitution does not address the issue of privacy, but two of its amendments do. As we will see in the next section, the Fourth Amendment directly addresses police invasions of privacy. As we will see later in this chapter, the Fifth Amendment addresses privacy indirectly by giving us a privilege not to cooperate with law enforcement evidence-gathering under certain circumstances.

Our review of the limits U.S. law places on police intrusions into private places and private activities will focus almost exclusively on these two provisions for several reasons, the most obvious of which is that they are the only constitutional provisions to deal with privacy. There are also federal and state statutes that deal with privacy, but we will consider them only briefly, for two reasons.

One reason is that these statutes either implement the Fourth Amendment and Fifth Amendment, which means reviewing them would be superfluous, or they are state laws that provide citizens with more protection than either or both amendments. State statutes that provide more protection than the Fourth and/or Fifth Amendments apply only to police conduct that occurs in the state that has adopted such a law. Therefore, these state statutes are of limited applicability. More importantly, these statutes are enforceable only against law enforcement officers who are employed by that state; they do not apply to federal law enforcement officers or to law enforcement officers from other states.

The other reason we will focus primarily on constitutional provisions and only incidentally on state and federal privacy statutes is that statutes are

much more fragile than constitutional provisions. It is not particularly difficult for Congress or for a state legislature to modify or even repeal a statute it adopted at some earlier time. Statutory law is inevitably unstable, in greater or lesser degrees. Astatute is in effect only unless and until the legislature that adopted the statute decides to change it or eliminate it.

On the other hand, it is very difficult to modify the U.S. Constitution. The only way to modify it is by amending it (i.e., by adding to it), and amendment is far from easy. Under Article V of the Constitution, there are two ways it can be amended.[7] One way is for two-thirds of both Houses of Congress to propose an amendment; the other way is for the legislatures of two-thirds of the states to ask Congress to convene a Constitutional Convention for the purpose of considering an amendment.[8] Once an amendment has been proposed by either means, it does not become part of the Constitution until it has been ratified by at least three-quarters of the U.S. states.[9] All the amendments that have been proposed so far came from Congress; the second method has never been used.[10]

The amendments we will examine are both part of the Bill of Rights, a set of 10 amendments that went into effect in 1791, after they were ratified by three-quarters of the states that then existed.[11] The Bill of Rights was added to the Constitution because some of those involved in drafting the Constitution feared the strong federal government it creates might become a threat to individual rights. The Bill of Rights was intended to emphasize that the rights it addresses are protected under the U.S. Constitution and therefore are binding on both the state and federal governments.

FOURTH AMENDMENT: BACKGROUND

The Fourth Amendment provides as follows: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." In the first section that follows, we will examine the evil the Fourth Amendment was originally intended to address. In the next two sections after that, we will examine how the Fourth Amendment has been—and should be—applied to technology that did not exist when it was adopted.

As is the case with much of our law, the Fourth Amendment derives from English common law. Early common law punished "those who invaded a neighbor's premises,"[12] and by the sixteenth-century, English law

criminalized burglary and trespass.[13] These laws were directed at private citizens because law enforcement searches of private property were almost unknown until the fifteenth century.[14] In the late fifteenth century, the king and Parliament began authorizing guilds to search property as a way of enforcing guild regulations.[15] Roughly a century later, the Court of the Star Chamber, which regulated printing, "decreed that the wardens of the Stationers' Company" had "authority to . . . search in any warehouse, shop, or any other place where they suspected a violation of the laws of printing to be taking place [and] seize the books printed contrary to law."[16] Other courts issued similar edicts authorizing searches targeting those suspected of heresy and political dissent.[17] This led to the evolution of the general warrant, which issued with no proof of individualized suspicion and in which no "names are specified . . . and . . . a discretionary power given to messengers to search wherever their suspicions may chance to fall."[18] As arbitrary searches became more common, "Englishmen began to insist that their houses were castles for the paradoxical reason that the castle-like security that those houses had afforded from intrusion was vanishing."[19]

In several cases from the mid-eighteenth century, English judges held that law enforcement officers could not arbitrarily search people's homes.[20] Most of the decisions resulted from an investigation into seditious libel.[21] Ordered to find the person who wrote a recently published seditious letter, officers armed with a general warrant searched five houses.[22] The people whose homes they searched sued the officers for trespass, and the British government defended them. To the delight of the British public, the plaintiffs won, and their verdicts were upheld on appeal.[23] Encouraged by their success, John Entick, the victim of a similar search, sued the officers who searched his home for trespass and won a verdict of £300.[24] The Court of Common Pleas upheld his verdict:

> Our law holds the property of every man so sacred that no man can set his foot upon his neighbour's close without his leave. If he does, he is a trespasser. . . . The defendants have no right to avail themselves of the usage of these warrants. . . . We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society.[25]

The cases applied the same standard to private citizens and law enforcement officers. Either could be held civilly liable for trespass if he entered someone's property "without a lawful authority."[26] The difference was that a law enforcement officer could rely on a warrant, as well as on a property owner's consent, as authorization for an entry.[27]

During this era, the American colonists were waging their own war against writs of assistance, a variant of the general warrant.[28] The colonists challenged the writs in court but lost,[29] and the failure generated resentment that was a driving factor in the Revolution and in the adoption of the Bill of Rights.[30] The Fourth Amendment was a product of the same concerns that resulted in the law of trespass being applied to public actors: "to guard individuals against improper intrusion into their buildings where they had the exclusive right of possession."[31] It was meant to secure spatial privacy—to restrict law enforcement's ability to break down doors and rummage through rooms, boxes, chests, drawers, and so forth. Similar to its English analogue, the Fourth Amendment was meant to ensure that law enforcement officers could legitimately intrude into someone's private places only if they had a valid search warrant—one based on probable cause to believe this particular person was involved in specific criminal activity.

General warrants gave officers essentially unlimited discretion; they could search wherever they liked, as often as they liked. Fourth Amendment search warrants limit an officer's discretion by requiring "individualized suspicion." To search a person or place, an officer must be able to cite "specific, articulable facts" that indicate evidence of a crime will be found at that place or on that person.[32]

For more than a century, courts had little difficulty applying the provisions of the Fourth Amendment because the conduct in which law enforcement officers engaged was essentially indistinguishable from what British and American officers had been doing for centuries: searching places and people. Privacy was still a matter of places: the inside of a home, the bed of a horse-drawn cart, or the contents of someone's pockets. As we will see in the next section, privacy became much more problematic in the twentieth century as new technologies began to erode the linkage between privacy and a spatial area.

Before we take up modern technologies, I need to note an 1877 U.S. Supreme Court decision that dealt with an aspect of what I call portable privacy. The issue was whether items traveling through the U.S. mail are private under the Fourth Amendment.

The case is *Ex parte Jackson*.[33] It involved Mr. Jackson appealing his conviction for sending "a circular concerning a lottery" through the mail.[34] In 1876, Congress made it a federal crime to "deposit in the mails any letters or circulars concerning lotteries"; the legislation was prompted by concerns that honest citizens were being "swindled" by crooked lotteries.[35] Jackson argued that the statute criminalizing the use of the mail to send lottery

materials was unconstitutional but lost on this issue. The Supreme Court held that Congress could prohibit the mail from being used to deliver certain types of material as long as the enforcement of the prohibitions complied with the Fourth Amendment:

> [A] distinction is to be made between . . . what is intended to be kept free from inspection, such as letters, and sealed packages . . . and what is open to inspection, such as newspapers . . . and other printed matter, purposely left in a condition to be examined. Letters and sealed packages . . . are as fully guarded from . . . inspection, except as to their outward form and weight, *as if they were retained by the parties forwarding them in their own domiciles.*[36]

In the Jackson case, the Supreme Court took its first step toward portable privacy, that is, toward the principle that the Fourth Amendment does more than prevent police from breaking into our homes and searching them without a valid warrant. The court would return to this issue roughly 50 years later in a case involving telephones.

FOURTH AMENDMENT: TELEPHONES

Alexander Graham Bell invented the telephone in 1876. By 1877, there were more than 30,000 phones in use around the world; by 1886, more than 250,000 were in use.[37] By 1898, the Bell Telephone Company had installed one million telephones in the United States. The installation and use of telephones continued its rapid expansion over the next 20 years, and by the 1920s, telephones were a routine feature of life, even in many rural areas.[38]

Police quickly realized that eavesdropping on telephone calls could be useful in investigating crime. Wiretapping was not new. During the Civil War, the Union and Confederate armies tapped each other's telegraph lines to gain information about troop movements and battles.[39]

Police had begun tapping telephone conversations at least by the 1890s.[40] Law enforcement wiretapping continued for years and became the focus of a controversy in 1916, when the public learned the phone company had been helping the New York City Police eavesdrop on calls.[41] The police claimed there was nothing improper about this because at the time, people had to go through an operator to place calls: "Telephone conversations . . . cannot be private in the way that letters can be, since the employees of the telephone company cannot help hearing parts of conversations and may, if they are inclined, easily hear all."[42] Basically, the New York City Police—similar to other police departments—viewed operator-assisted phone calls as the oral

equivalent of sending a postcard through the mail. Similar to a postcard, a telephone call placed through an operator was not, in fact, private.

By the 1920s, automatic switching systems had eliminated the need to rely on an operator to place a call.[43] With automated switching, we dial a number, and the phone company's technology connects the call, without human involvement. As automated switching became increasingly common, people began to assume phone calls were private, in the same way that sealed mail is private.[44] People therefore began to use phones more and more, and that brings us to Roy "Big Boy" Olmstead.

On January 16, 1920, the Eighteenth Amendment to the U.S. Constitution went into effect. Along with the National Prohibition Act, it outlawed the "manufacture, sale, transportation," and importation of "intoxicating liquors" in the United States.[45] Ironically, Prohibition gave rise to an increased demand for liquor in the United States, and a new profession arose: bootlegger. Everyone has heard of Al Capone, who made millions selling illegal alcohol, but almost no one knows about Roy "Big Boy" Olmstead, who would play an important role in shaping how the Fourth Amendment applies to telephone calls.

When Prohibition went into effect, Olmstead was a respected lieutenant in the Seattle Police Department.[46] As a police officer, Olmstead was involved in raids on the bootleggers, who cropped up almost as soon as Prohibition went into effect. He noted the bootleggers tended to have a lot of money and to get caught because their operations were not well organized. Attracted by the money, Olmstead decided to become a bootlegger and quickly became the head of a large, complex organization that smuggled alcohol into the United States from Canada. His gang operated unimpeded for four years because there were few Prohibition agents, and it was virtually impossible to catch smugglers in the Pacific Northwest: "There was too much border, too much water, and too many islands . . . to patrol effectively."[47]

By 1924, federal Prohibition agents were investigating what had become a very visible bootlegging operation that brought in $2 million a year at its peak.[48] In addition to using traditional investigative methods such as snitches, the Prohibition agents put wiretaps on a number of telephones being used by the Olmstead gang, including the telephone in Olmstead's home. Agents spent months listening to conversations between Olmstead and other members of his gang. They used what they had heard—and had transcribed by a stenographer—to get a warrant to search Olmstead's home. On November 24, 1924, they raided Olmstead's home and seized the

organization's records." On January 25, Olmstead and 89others were indicted on two counts of violating federal Prohibition laws.

Olmstead went to trial and was convicted. He appealed a single issue all the way to the U.S. Supreme Court: "whether the use of evidence of private telephone conversations between [Olmstead] and others, intercepted by means of wire tapping, amounted to a violation of the" Fourth Amendment.[49] In its opinion, the Supreme Court described how the wiretapping was carried out:

> Small wires were inserted along the . . . telephone wires from the residences of four [conspirators] and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.[50]

Olmstead argued that what the Prohibition agents did was a search because they listened in on conversations that occurred in private places: his home and those of three other members of his gang plus the office the gang used as its headquarters. Olmstead was arguing that the agents effectively did the same thing the British officers did when they searched Entick's home; they violated the sanctity of homes and another private place without having first obtained a search warrant.

Olmstead's argument may strike us as compelling, but most of the members of the court that heard his appeal were born and educated in the nineteenth century and therefore did not understand how technology can alter traditional conceptions of privacy. These Justices held that the use of technology was irrelevant because the "Fourth Amendment is to be construed in the light of what was deemed an unreasonable search . . . when it was adopted."[51] They went on to hold that because the Prohibition agents had not physically entered the homes or the office, there was no search:

> [O]ne who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and . . . the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.
>
> We think, therefore, that the wire tapping here . . . did not amount to a search . . . within the meaning of the Fourth Amendment.

Justice Louis Brandeis dissented. Similar to his colleagues, Brandeis was a product of the nineteenth century; unlike them, he was able to grasp the

significance of this new technology. In his dissent, he wrote that when the Fourth Amendment was adopted, the only way the government could "secure possession of [the] papers and other articles incident to [someone's] private life" was by "breaking and entry" into the person's home or office.[52] He explained why the majority of the court was wrong when it insisted that the Fourth Amendment was set in stone, that is, was to be interpreted as if the world had not changed in the years since it was adopted:

> [I]n the application of a Constitution, our contemplation cannot be only of what has been, but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may . . . be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose . . . the most intimate occurrences of the home. . . . That places the liberty of every man in the hands of every petty officer.

Justice Brandeis would have applied the Fourth Amendment to the wiretapping in the Olmstead case, which would have meant the evidence would have been suppressed; unfortunately, he did not prevail. Olmstead went to jail and for the next almost 40 years, telephone conversations were not protected by the Fourth Amendment.

In 1965, the FBI was investigating Charles Katz, a bookie who operated in Los Angeles, for violating federal gambling law.[53] As the agents surveilled Katz, they realized he always used one of three phone booths in the 8200 block of Sunset Boulevard to make calls concerning bets; the agents put microphones and recording devices on the top of all three phone booths and spent a week intercepting and recording all the calls he made. The intercepted calls were used to convince a grand jury to indict Katz on federal gambling charges. They were also used to convict him of those charges at his trial.

Prior to trial, Katz moved to suppress the transcripts of the intercepted calls, arguing that the interceptions were illegal searches under the Fourth Amendment. Because the Olmstead court had held wiretapping was not a Fourth Amendment search, the FBI agents had not gotten a warrant before installing the microphones and recorders. The trial court denied Katz's motion, and the Ninth Circuit Court of Appeals upheld the denial. Similar to the majority of the Olmstead Justices, these judges all held that there was no search because the agents put the recording devices on the outside of the phone booths. Because the agents did not trespass into the phone booths when Katz was in them, these judges held that there had been no Fourth Amendment searches.

The Supreme Court agreed to hear Katz's appeal and reversed the decision of the lower courts. The Katz court began its opinion by noting that the lower courts' focus on whether there had been a trespass into a physical space focused on the wrong issue because "the Fourth Amendment protects people, not places."[54] It also explained that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection, . . . but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." In a concurring opinion, Justice Harlan explained how courts are to determine whether something is, in fact private, under the Fourth Amendment:

> [T[here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is . . . a place where he expects privacy. . . . On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[55]

The Supreme Court found Charles Katz had a reasonable expectation of privacy in the phone booths. He believed his calls were private because he went into the phone booth and closed the door. The court also found that we, as a society, would consider that belief to be reasonable. The court therefore overruled the Olmstead decision, and intercepting telephone calls became a search under the Fourth Amendment, which meant officers must obtain a search warrant before conducting such an interception.

The Katz case was the first of two decisions the Supreme Court has issued on the applicability of the Fourth Amendment to telephone technology. The other decision came in 1979.[56]

On March 5, 1976, Baltimore resident Patricia McDonough was robbed. She gave the police a description of the robber and a 1975 Monte Carlo automobile she saw near the scene of the crime. Patricia began to receive "threatening and obscene" calls from a man who said he was the robber. At one point, he called and asked her to go out to her front porch. When she did, she saw the Monte Carlo driving slowly by her home. A few days later, police saw a man matching her description of the robber driving a car that matched her description of the Monte Carlo. They used the license plate number to trace the car to Michael Lee Smith. The next day, officers had the telephone company install "a pen register at its central offices to record the numbers dialed from the telephone" at Smith's home. The officers did not get a search warrant authorizing installation of the pen register; they simply asked the phone company to install it, and the phone company complied.

The pen register did not—could not—capture the contents of the calls Smith made. All it could do was to record the numbers he dialed from his home phone.

The day after the pen register was installed, Smith called Patricia, and the pen register recorded him dialing her number. Police used that and other evidence to get a warrant to search Smith's home, where they found evidence implicating him in the robbery. After he was indicted for robbery, Smith moved to suppress the evidence recorded by the pen register on the grounds that using it to discover the phone numbers he dialed from home was a search under the Fourth Amendment. Similar to Katz, Smith lost at the lower court level; the trial court and the Maryland Court of Appeals both held that using the pen register was not a Fourth Amendment search.

Smith appealed to the Supreme Court, which agreed to hear the case. Unlike Katz, he lost. The court applied the standard Justice Harlan articulated in the Katz ruling and found Smith did not have a reasonable expectation of privacy in the numbers he dialed from his home phone. The court found, first, that Smith could not have believed the numbers he was dialing were private because he knew he was "giving" them to the phone company: "All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[57]

The court also held that even if Smith subjectively believed the numbers he dialed were private, this was not a belief society accepts as objectively reasonable: "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[58] In making that statement, the court cited a case decided a few years earlier, in which it held that bank customers have no Fourth Amendment expectation of privacy in information they share with their bank:

> [C[hecks are not confidential communications but negotiable instruments to be used in commercial transactions. . . . [F]inancial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. . . .
>
> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.[59]

The Katz and Smith decisions mean that the applicability of the Fourth Amendment to our use of telephones is governed by a dichotomy: If the government engages in conduct analogous to what it did in the Katz case (i.e., intercept the contents of phone calls as we make them), that will be a Fourth Amendment search under the Katz ruling. If the government uses the modern equivalent of pen registers and trap and trace devices (which capture the phone numbers of people who call a particular phone[60]) to record the phone numbers we call and the phone numbers of the people who call us, that is not a search under the Smith decision.

Many, myself included, believe the Supreme Court got it right in the Katz case but got it very wrong in the Smith case. Justice Marshall wrote a dissent in the Smith case in which he, similar to Justice Brandeis in the Olmstead case, pointed out the flaw in the majority's reasoning. Justice Marshall took issue with the majority's holding that Smith, similar to a bank depositor, assumed the risk the phone company would reveal the information he shared with it to the government. He noted that "[i]mplicit in the concept of assumption of risk is some notion of choice."[61] He then pointed out that "unless a person is prepared to forego use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[62] Similar to Justice Brandeis and unlike his colleagues, Justice Marshall understood that communications technology had already become an intricate component of everyday life.

Unfortunately, the Supreme Court has never revisited—and therefore never reversed—its decision in the Smith case. The Katz and Smith dichotomy has become increasingly difficult to apply as technology has advanced far beyond what it was when the Smith decision was made. Some of the difficulties involve advanced telephone technology. However, as we will see in the next section, most of them—the most problematic of them —involve evolved communications technologies such as e-mail.

FOURTH AMENDMENT: COMPUTER TECHNOLOGY

Computer technology raises a number of Fourth Amendment issues, but none is more intimately entwined with personal privacy than the applicability of the Fourth Amendment to online communications: e-mail and other messages, the comments and information we post on Web sites, and data generated by our online transactions. In the following sections, we examine the Fourth Amendment issues each type of communication presents.E-mail

Because the same issues arise for e-mail, texts, and instant messages and because e-mail has been the primary focus of Fourth Amendment litigation, we will concentrate on it. In deciding the extent to which e-mail is "private" and therefore protected by the Fourth Amendment, courts must decide which of the Supreme Court cases we previously examined govern e-mail:

Is it a phone call (the Katz case), a letter (the Jackson case), or the equivalent of giving financial information to a bank or phone numbers to the phone company (the Smith case)?

In making that decision, courts must deal with the fact that similar to a letter or a phone call, e-mails involve two types of information: the contents of the message and the data that are used to transmit the message from the sender to the recipient. The former is known as "content data" and the latter as "traffic data."[63] We will begin by analyzing the extent to which the Fourth Amendment applies to content data and then consider traffic data.

If we analogize e-mail to a sealed letter, the content data are the substance of the communication—the digital equivalent of what is written on a letter inside an envelope. The traffic data are the addressing information used to send it—the digital equivalent of the names and addresses written on the outside of the envelope. If that analogy is correct, then under the Supreme Court decision in the Jackson case, the Fourth Amendment protects the contents of an e-mail but not the traffic data used to send it. This would mean that law enforcement officers could not access the contents of an e-mail in the process of being sent unless they first obtain a search warrant. (In a moment, we will get to e-mails that have arrived and are being stored in someone's e-mail account.)

I suspect most Americans assume this analogy is correct and their e-mails are immune from law enforcement inspection unless and until officers get a warrant that lets them read one or more e-mails. There is, however, a problem with the analogy. In the Jackson ruling, the Supreme Court emphasized that the Fourth Amendment applies to sealed letters because the sender took steps to prevent postal employees from reading them. This premise is consistent with the Katz ruling. Under the Katz ruling, the Fourth Amendment protects the contents of sealed letters because by sealing the envelope, the sender makes an effort to keep the contents of the letter private and therefore does not assume the risk that it will be read by postal employees. The Jackson court also held that the Fourth Amendment does not protect items that are not sealed—newspapers and postcards—because the sender has assumed the risk that others will read them as they travel through the mail.

That brings us back to e-mails. To be analogous to a letter, an e-mail must be sealed, that is, the sender must do something to prevent its being read as it travels to its intended recipient. The only way to seal an e-mail is to encrypt it, but almost no one (outside the military and intelligence communities) encrypts e-mails for two reasons. One reason is that encrypting e-mail tends to be a complex, cumbersome process; the other reason is that most people—certainly most Americans—assume e-mail is already private,so there is no need to encrypt. Most Americans, in other words, assume an e-mail is the equivalent of a sealed letter; it will not be read by anyone except its intended recipient.

That, though, is not true. ISPs can, and do, scan the contents of at least some of the e-mails sent via their systems.[64] The same is true of noncommercial providers such as universities.[65] E-mail providers screen e-mails in an effort to prevent their systems from being used for illegal purposes, but they are not the only ones who can read e-mails as the messages travel through a system. The employees of an ISP or other provider can read unencrypted e-mails in the same way that a postal employee can read a postcard.[66] Because of that, some, including the U.S. Department of Justice, claim the Fourth Amendment does not protect unencrypted e-mail. In a recent case, the Justice Department argued that e-mail "resembles less a sealed letter than a postcard amenable to warrantless inspection, because 'its contents are plainly visible to the [ISP], who can access it via its servers at any time.' "[67]

I suspect most of us do not agree with this position, but it is difficult to distinguish unencrypted e-mail from a postcard. We have not, as the court in the Jackson case put it, sealed the message to keep it from prying eyes. Therefore, we have, as the court in the Katz case would say, assumed the risk that employees of our ISP will read our e-mail. Unless and until the Supreme Court takes up this issue and holds that unencrypted e-mail is somehow more private than a postcard, it is prudent to assume that unencrypted e-mail is outside the protection of the Fourth Amendment.[68] If that is true, it means that if an ISP scans e-mail and finds evidence of a crime, it can turn the e-mail over to law enforcement officers without the officers having to get a search warrant.[69] It might also mean officers could ask an ISP to scan someone's e-mail and report what it finds, without getting a search warrant.[70]

There is another way to argue that the contents of e-mail—even unencrypted e-mail—are protected under the Fourth Amendment. It analogizes e-mails to phone calls instead of letters (or postcards). In 1968, Congress adopted a statutory scheme to implement the Supreme Court decision in the Katz case. Known as Title III (because it was the third title of a larger, more comprehensive bill), this legislative scheme requires officers to obtain a warrant before intercepting telephone calls and to otherwise comply with the requirements of the Fourth Amendment. In 1986, Congress expanded Title III so that its provisions also apply to the interception of e-mail; Congress wanted to ensure that this new medium of communication was also protected from arbitrary eavesdropping.[71]

Under Title III, law enforcement officers use the same procedure to eavesdrop on telephone calls and to intercept the contents of e-mails that are in

the process of being transmitted from a sender to a recipient.[72] Because Title III is a statute rather than a Supreme Court decision, it does not extend Fourth Amendment protection to the contents of e-mail.[73] It does, however, support an argument for analogizing e-mails to phone calls: Similar to ISPs, phone companies can, and do, listen in on calls.[74] Notwithstanding that, the court in the Katz case held that we have a Fourth Amendment expectation of privacy in our phone calls.[75] If the communication service provider's ability to intercept the content of communications does not defeat a Fourth Amendment expectation of privacy in phone calls, then it should not defeat such an expectation with regard to the content of unencrypted e-mails. So far, no court has ruled on this issue, although a federal court of appeals noted in passing that it found the argument "convincing."[76] The issue has presumably not arisen because state and federal law enforcement officers assume they must comply with the requirements of Title III in order to obtain any e-mails (encrypted or unencrypted) lawfully.

A related issue has come up, most notably in the federal court of appeals case I noted earlier: whether the Fourth Amendment protects the contents of e-mails once they arrive at their destination and are stored on the ISP servers. This issue does not arise for telephone calls because the only way the government can acquire the contents of a phone call is to capture the conversation as it occurs. The creation and transmission of the content occur simultaneously, and the content exists only momentarily.[77] E-mails, on the other hand, are stored on an ISP server for some period of time after they arrive and until we read them. After we read e-mails, many of us keep them in a file in our e-mail account. This means that the government has an additional way to obtain the content of e-mails: Law enforcement officers can ask an ISP to copy the archived e-mails and give the copies to the officers. If the archived e-mails are protected by the Fourth Amendment under the Katz or Jackson cases, then the officers must get a search warrant to obtain copies of the e-mails. If the e-mails are not protected by the Fourth Amendment, then officers can simply ask for the copies and the ISP can, if so inclined, create them and turn them over to the officers.

This was the issue in the case I noted earlier: In 2005, federal agents were investigating Steven Warshak for "mail and wire fraud, money laundering and related federal offenses."[78] As part of the investigation, the agents obtained copies of e-mails Warshak had archived in his Yahoo! e-mail account. The agents did not use a search warrant. Instead, they relied on a procedure in another statutory scheme—the Stored Communications Act (SCA)—to obtain the e-mails. Under the SCA, officers can obtain the

contents of stored e-mails by getting a judge to order an ISP to copy the e-mails and give the copies to the officers.[79] Unlike a magistrate issuing a search warrant, the judge who issues such an order does not have to find there is probable cause to believe the e-mails are evidence of a crime.[80] The SCA procedure therefore does not comply with the requirements of the Fourth Amendment and is unconstitutional if the Fourth Amendment protects the privacy of e-mails that are stored on an ISP server.

As I noted earlier, stored e-mails are not analogous to the phone call at issue in the Katz case; they consist of text and are acquired after the message has been received. Although they are, to some extent, analogous to the mail at issue in the Jackson case, we use the mail only to transmit letters; we do not store read letters with the U.S. Postal Service. That leaves the Smith decision. The Supreme Court has not addressed this issue, but the Department of Justice and others believe stored e-mail comes under the Smith holding, that is, data we share with a third-party loses its Fourth Amendment protection. The SCA is based on this proposition. The assumption is that the SCA gives some protection to stored e-mails, which would otherwise be available to law enforcement on demand. Under the Smith ruling, by leaving e-mails stored on our ISP servers, we assume the risk that the ISP will give copies of those e-mails to law enforcement officers, even without a search warrant.

Steven Warshak challenged this view; he sued the Department of Justice for violating his rights by obtaining his stored e-mails without a warrant. Warshak relied on the argument outlined previously, that is, because the ability of the phone company to listen in on phone calls does not deprive calls of Fourth Amendment protection, the ability of an ISP to read stored e-mails should not deprive them of Fourth Amendment protection. A federal district court agreed with him, and so did a three-judge panel of the U.S. Court of Appeals for the Sixth Circuit. For a few months, the Fourth Amendment protected the contents of all e-mails. The Department of Justice was not pleased with this ruling because it meant officers and agents had to get a search warrant to obtain stored e-mails. So the Justice Department appealed the decision of the three-judge panel to the entire Court of Appeals for the Sixth Circuit in what is called an *en banc* procedure, and that court blinked.

The *en banc* court ducked the issue by using a technical rule to hold that the case was not "ripe" for review by the courts.[81] The *en banc* court said the lower courts should not have entertained Warshak's claims because there was no live controversy. Warshak had already been indicted, and there was no indication the government would seek further copies of his e-mails from Yahoo! The *en banc* court therefore vacated the opinions of the lower courts,

which means they ceased to have any legal effect. One of the judges dissented, pointing out the fallacy in the majority's reasoning and noting the importance of the issue that would be left undecided:[82]

> If I were to tell James Otis and John Adams that a citizen's private correspondence is now . . . subject to ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless.

If the *en banc* Warshak court had agreed with the lower courts, the issue would almost certainly have gone to the Supreme Court because the Department of Justice would have asked the Supreme Court to reverse the lower courts. By holding there was no controversy, the *en banc* court prevented that and put an end to this attempt to apply the Fourth Amendment to the content of stored e-mails. As a result, we remain, where we were before Warshak sued. The assumption is that stored e-mails are governed by the Smith holding and therefore are not protected by the Fourth Amendment.

The information used to transmit e-mail—the "to" and "from" fields in an e-mail plus the data an e-mail generate as it moves through a series of mail servers to its final destination[83]—is clearly not protected by the Fourth Amendment. E-mail traffic data are logically indistinguishable from the numbers we dial to place phone calls. In both instances, we surrender Fourth Amendment privacy by sharing that information with a third party.

Web Postings

Under the Katz ruling, the Fourth Amendment does not protect any content we post on a publicly accessible Web site. As the court said in the Katz decision, what we knowingly expose to public view is not private. Because anyone can access the site and see what we posted, law enforcement officers can do the same without obtaining a search warrant. Officers can, and do, use postings on MySpace and other Web sites in investigating criminal activity.[84]

What if the site is password-protected? That was the issue in *United States v. D'Andrea*,[85] a federal prosecution for sexually abusing a child. On December 2, 2004, an anonymous woman called a child abuse hotline and said the eight-year-old daughter of Kendra D'Andrea "was being sexually abused by her mother and the mother's live-in boyfriend." She said they had posted photographs of the abuse on a password-protected Web site and provided the log-in name and password needed to access the site. A child abuse

investigator used the information to log into the site, where he found photos of a child being sexually abused. He downloaded the images and called the police, who used the images and the information from the caller to get a warrant to search D'Andrea's apartment. When they executed the search warrant, they found information that further incriminated D'Andrea and her boyfriend.

After being charged with sexually abusing a child, D'Andrea moved to suppress the images the investigator downloaded from the password-protected site. She said the investigator violated the Fourth Amendment by accessing the site and downloading the images without first getting a search warrant. D'Andrea claimed the site was protected by the Fourth Amendment because only those who knew the log-in name and password could access it. She argued that by using a password and log-in name, she ensured the privacy of the Web site, just as Charles Katz ensured the privacy of his phone calls by using a phone booth. In ruling on this issue, the federal district court noted that the leading expert on Fourth Amendment law believes "that a person who avails herself of a website's password protection should be able to claim a reasonable expectation of privacy in the site's contents."[86]

Although the judge found this view persuasive, he concluded that he did not have to decide this issue because the investigator did not break into the site (i.e., did not bypass the measures D'Andrea used to secure it). He used the login information the anonymous caller provided to access the site. Because she was not a law enforcement officer (she was a former girlfriend of D'Andrea's boyfriend), the Fourth Amendment did not apply to her. Similar to any private citizen, she was free to share information with the police. By sharing the login information with this person, D'Andrea assumed the risk she would give it to the police. As the Supreme Court said in *United States v. Jacobsen*,[87] "when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." Although D'Andrea almost certainly created a Fourth Amendment expectation of privacy in the site by password-protecting it, she lost that right by giving the log-in information to someone who gave it to the police.

Like others, I believe that password-protecting a Web site creates a reasonable expectation of privacy in the contents of that site and therefore requires law enforcement to obtain a search warrant to access the contents of the site without the owner's permission. Password-protecting a site should trigger full Fourth Amendment protection. If the owner of the site shares login information for the site with someone, he assumes the risk that this person

will betray him by sharing that information with law enforcement. This means the only way that someone can sustain Fourth Amendment protection for a password-protected site is by not sharing login information for the site with anyone else.

Transactions

When we surf the Web, shop online, or engage in any other type of online activity, we leave a record of where we have been and what we have done. We may be alone in a private, locked room while we do any or all of these things and therefore assume that what we are doing is private, but that is not true. We are more visible online than we are in the real, physical world.

If law enforcement wants to track our activities in the real world, it will have to assign officers to monitor our movements in public and to interview witnesses who can describe what we were doing in private places. Law enforcement officers can install and use certain technologies such as GPS tracking devices to keep track of where we go in our vehicles, but beyond that, they will have to use officers to monitor our movements. Because that is a time-consuming and resource-intensive process, law enforcement can track only a few of us at any one time.

Monitoring what we do online is much easier. Technology keeps track of every site we visit and every action we take on each site. It also keeps a record of that activity, which will be stored with our ISP and/or with the operators of the sites we visit. This information can be very useful for law enforcement officer. For example, federal agents investigating the possibility that a suspect is planning a terrorist bombing could use the records of his Internet activity to find out if he is trying to buy explosives or researching how to build a bomb. If he is using the Internet, there will be records showing what sites he visited and what he did on those sites.

Is that information protected by the Fourth Amendment? If it is, then the agents will have to obtain a search warrant to gain access to it. To obtain a search warrant, they must convince a magistrate they have probable cause to believe this person is planning a terrorist bombing. That is not an impossible task, but it means the agents will not be able to obtain the online records early in their investigation; they will have to wait until they develop the necessary probable cause from other sources. If the Fourth Amendment does not protect the information, the agents can obtain it without getting a search warrant; they could simply ask the suspect's ISP and the Web sites to provide it. If the ISP and/or Web sites refuse, the agents can use a subpoena

—a judicial order that commands the recipient to take certain action or be held in contempt[88]—to require the ISP and/or Web sites to comply. Unlike a search warrant, a subpoena issues without a showing of probable cause to believe evidence of a crime is in a particular place.[89]

A few courts have considered whether the Fourth Amendment protects the data we generate when we shop or do anything else in the public areas of cyberspace. In *United States v. Forrester*,[90] for example, federal agents installed a "mirror port"—the twenty-first century equivalent of a pen register—on Louis Alba's account with an ISP. The agents suspected Alba and Forrester were involved in manufacturing Ecstasy, a controlled substance.

They used the mirror port to monitor "the IP addresses of the websites that Alba visited." An Internet Protocol (IP) address is "a numerical identification . . . that is assigned to" Web sites and other "devices in a computer network."[91] Google has many different IP addresses, one of which is, or was, 216.239.51.99.[92] To access Google or any other site, we do not use the numerical IP address; instead, we use a domain name, a pattern of text that our computer translates as a request to access an IP address and implements.[93] In the Forrester case, the federal agents used the mirror port installed on Alba's account with his ISP to track the Web sites Alba visited, in the same way officers in the Smith case used a pen register to capture the numbers Smith dialed from his home phone.

In the Forrester case, the evidence the mirror port compiled was used to indict Alba for violating federal drug laws and to convict him on those charges. He appealed his conviction, arguing that the use of the mirror port violated the Fourth Amendment. The U.S. Court of Appeals for the Ninth Circuit disagreed:

> [T[he surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. . . . Internet users, like the telephone users in Smith, rely on third-party equipment to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. . . . Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit because they should know this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," . . . IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.[94]

As long as the Smith decision is a valid precedent, courts cannot reach any other conclusion.

Unless and until the Supreme Court revisits this issue and overrules the Smith decision, the data we generate when we are online are outside the Fourth Amendment. In other words, the data are not private. That has certain consequences, one of which is that law enforcement officers can track our online activity in real time or retroactively without getting a search warrant. This use of online data is simply an extension of traditional investigative methods. As such, it usually focuses on one individual or only on one individual at a time.

The Smith decision not only supports this traditional investigative methodology, it creates the possibility of a new investigative methodology: data mining. Data mining consists of compiling massive amounts of information in databases and then analyzing it to identify patterns that are not ascertainable otherwise.[95] Because the Smith ruling puts the information we share with third-parties outside the scope of the Fourth Amendment, it creates the possibility that law enforcement can compile this information in databases and use sophisticated programs to analyze it and identify patterns officers can use to commence and conduct investigations. Not surprisingly, law enforcement is interested in this possibility. Some data mining efforts, such as the unfortunately named MATRIX project,[96] have been implemented, but most have not been successful, due in part to concerns about privacy.

That does not mean such efforts will not succeed in the future. As long as the Smith decision stands, there is no constitutional impediment to a process the drafters of the Bill of Rights would certainly have found objectionable. As long as the Smith decision survives, Fourth Amendment privacy and the use of modern communications technologies are irreconcilable. I cannot use any communication technology without sharing information with a third-party, which leaves the information unprotected by the Fourth Amendment. I believe Justice Marshall was correct when he argued in his dissent with the Smith ruling that the result in that case creates a technological Hobson's choice: If I use technology, I lose privacy; to have privacy, I must give up technology. I suspect most, if not all, of us would agree with Justice Marshall that this is a choice we should not have to make.

There is a way we can invoke Fourth Amendment protection for our online activities. As we have seen, the Fourth Amendment presumably protects encrypted e-mails because we have, in effect, sealed the envelope. Encryption can also be used to protect other online activities and to secure hard drives and other data storage devices,[97] thereby making it difficult or even impossible for law enforcement to access the data they contain. As we will see in the next section, law enforcement can try to compel us to give up the key needed to access encrypted data or devices, but the Fifth Amendment may give us the ability to resist such efforts.

FIFTH AMENDMENT

Similar to the Fourth Amendment, the Fifth Amendment is part of the Bill of Rights—the first 10 amendments to the Constitution. It contains several clauses, each of which establishes a distinct right. For example, one clause creates the prohibition against double jeopardy (i.e., against trying someone twice for the same crime).

Our concern is with the clause that says "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." Similar to the Fourth Amendment, this clause has its roots in English law and history. In the sixteenth and seventeenth century, two powerful English courts—the Court of High Commission and the Court of Star Chamber—used a procedure called the oath ex officio to bring people into court and force them to answer questions that could implicate them in crimes "of which they were neither formally accused nor suspected."[98] If someone refused to take the oath ex officio or, having taken it, refused to answer questions, he or she would be punished. For example, the Court of Star Chamber ordered John Lilburne to be "whipt through the streets, from the prison of the Fleet unto the pillory" for refusing to comply.[99] In 1641, Parliament outlawed the use of the oath ex officio, prompted by complaints from citizens who said no one should be forced to testify against himself or herself. The theory was that people had a right not to be compelled to betray themselves—that the government should collect its own evidence instead of forcibly extracting what it needed from a suspect. English colonists brought that notion to what would become the United States, and it was eventually incorporated into the Fifth Amendment.

The Fifth Amendment clause with which we are concerned is known as the privilege against self-incrimination because it operates in the same way as an evidentiary privilege (i.e., it gives someone the privilege of refusing to testify). In that regard, it is similar to the marital privilege (i.e., one spouse cannot be forced to testify against the other) or the attorney-client privilege. The Fifth Amendment is not, as the Supreme Court has explained, a privilege that bars the government from asking someone questions; it simply gives the person the ability to refuse to answer those questions.[100] The Fifth Amendment gives us an option that was not available to those summoned before the Court of Star Chamber: Their only options were to answer

truthfully (implicating themselves in a crime), lie (committing perjury and condemning their souls to eternal damnation), or refuse to answer and be punished. The Fifth Amendment gives us a fourth option: refuse to answer and suffer no consequences for doing so.

However, the privilege is available only in certain circumstances. To be able to invoke the Fifth Amendment privilege, a person must be compelled to give testimony that incriminates him (implicates him in a crime).[101] If someone is willing to testify voluntarily, there is no need for compulsion, and the Fifth Amendment does not apply. It usually comes into play when the government wants someone to testify at a trial or a grand jury proceeding, but that person refuses. The government can use a subpoena—a trial subpoena or a grand jury subpoena—to force the person to appear. If someone who was served with a subpoena shows up at the trial or grand jury proceeding and refuses to answer questions, he will be held in contempt and incarcerated until he agrees to testify . . . unless he can invoke the Fifth Amendment privilege.

The subpoena satisfies the first requirement because it compels the person to testify (absent a claim of the privilege). The second requirement limits the application of the privilege to testimony (i.e., to communicating facts or opinions). The Supreme Court has held that the Fifth Amendment does not apply to physical evidence, which means we can invoke the privilege and refuse to answer questions posed by a prosecutor, but we cannot invoke it to refuse to let the government take samples of our blood or hair. If the prosecutor is using the subpoena to get the witness to answer questions, then the person will be able to invoke the Fifth Amendment privilege if answering the questions will incriminate him or her (i.e., will implicate him in criminal activity). The Fifth Amendment is not a privilege to refuse to speak; it is a privilege to refuse to be a witness against yourself (i.e., to give testimony that can be used to prosecute you for a crime). That brings us to Sebastien Boucher.

On December 27, 2006, Sebastien Boucher and his father crossed the Canadian border into the United States at Derby Line, Vermont.[102] Like everyone entering the United States, they were subjected to an initial inspection of their passports; however, unlike most who enter the United States, the Bouchers were selected for secondary inspection. If the federal agent who conducts the initial inspection thinks the traveler is carrying contraband, he will refer the person for a secondary inspection, which involves searching the person's luggage.

As Officer Pike conducted the secondary inspection, he saw a laptop in the car, booted it up, and looked through the files it contained. Pike found

40,000 image files, "some of which appeared to be pornographic based on the names of the files." He asked Sebastien if there was child pornography on the laptop; Sebastien said he was not sure. Sebastien said he downloaded pornography and sometimes his downloads included child pornography; Sebastien said he deleted those images when he found them.

At that point, Pike called Agent Curtis for assistance because he had experience with locating digital child pornography. Curtis asked Sebastien to show him where the downloaded files were. Sebastien was given access to the laptop and "navigated to a part of the hard drive designated as drive Z." Curtis began looking through the Z drive and saw what he believed was child pornography. After searching further, Curtis arrested Boucher, shut down the laptop, and seized it as evidence. Two days later, another officer took custody of the laptop and began conducting a forensic examination of it. When he tried to access the Z drive, he could not because it was encrypted "through the use of the software Pretty Good Privacy . . . which requires a password." Curtis and a Secret Service agent tried repeatedly to access the Z drive but could not. According to the Secret Service agent, the only way to access the drive without having the password "is to use an automated system which repeatedly guesses passwords." The agent noted that "the process to unlock drive Z could take years based on efforts to unlock similarly encrypted files in another case."

Because it was clear that the only way to access the Z drive was with the password and that Boucher would not voluntarily provide the password, the government resorted to a subpoena. A federal grand jury served Sebastien with a subpoena that ordered him to enter the password into the laptop or be held in contempt. Boucher took the Fifth Amendment, claiming that providing the password would be compelled testimony that incriminated him. The Department of Justice argued that the password was physical evidence, not testimony, and so claimed Sebastien was not entitled to take the Fifth Amendment as the basis for refusing to enter the password.

In responding to this argument, Sebastien relied on the Supreme Court case of *Fisher v. United States*.[103] In that case, the court held that while someone cannot claim the Fifth Amendment privilege as the basis for refusing to provide physical evidence such as hair samples because physical evidence is not testimony, someone subpoenaed by a grand jury can invoke the Fifth Amendment if the act of producing the evidence would itself be testimonial. The court in the Fisher case said the act of producing evidence is a testimony within the Fifth Amendment if it concedes that the evidence exists, that the subpoenaed person has it, and that the evidence produced is what the grand jury asked for (i.e., producing it authenticates it). The court in the Fisher case

also said that the act of producing evidence will not be testimonial if all of these are a "foregone conclusion" (i.e., if the government already knows the person has the evidence).

When I teach the Fisher case, I use this example to illustrate when the act of producing evidence will be testimonial and when it will not: If a grand jury issues a subpoena to a murder suspect that demands she "produce to the grand jury the gun you used to kill Martin Balco," she can take the Fifth Amendment and refuse to comply. By handing over the gun, she is implicitly saying that it exists, that she has it, and that this is the gun she used to kill Balco. On the other hand, if the grand jury knows the suspect has the gun that was used to kill Balco (e.g. they have videotape of her buying it or one of her friends saw it and heard her say, "This what I used to kill Balco"), then handing it over does not tell the government anything it does not already know. If the act does not communicate anything, it is not testimonial, and she cannot take the Fifth Amendment.

In the Boucher case, the federal magistrate judge who was assigned to decide the issue held that giving up the password was a testimonial and incriminating act:

> Compelling Boucher to enter the password forces him to produce evidence that could . . . incriminate him. . . .
>
> Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing . . . that he knows the password and has control over . . . drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?"[104]

The judge therefore quashed the grand jury subpoena (i.e., withdrew it). Because it could not compel Sebastien to provide the password, the only way the government could get it was to give him immunity from prosecution, but it was not willing to do that. Giving him immunity would defeat the purpose because it would mean that none of the files on the laptop could be used to prosecute Sebastien for child pornography or any other crime.

The Department of Justice instead chose to appeal the magistrate judge's decision to the federal district judge who presides over the U.S. District Court for the District of Vermont.[105] It also decided to change tactics somewhat. In its appeal to the district judge, the Justice Department said it was not asking Sebastien to provide "the password for the encrypted hard drive, but . . . to produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury."[106] The Department of Justice also argued that Sebastien could not take the Fifth Amendment as to the contents of the laptop because they were a foregone conclusion under the Fisher ruling.

The Department of Justice won. The magistrate judge had decided the foregone conclusion principle did not apply in this case "because the government has not viewed most of the files on the Z drive, and therefore does not know whether most of the[m] . . . contain incriminating material." The district court judge disagreed; he found that for the foregone conclusion principle to apply, the government does not have to be "aware of the incriminatory *contents* of the files"; all it needs to know is that they exist in a particular location. The judge pointed out that the government knew this because Agent Curtis had looked through parts of the Z drive and had seen files, some of which appeared to be child pornography. The district court judge also held that Sebastien producing an unencrypted version of the hard drive would not authenticate it or the files on it because "he has already admitted to possession of the computer, and provided the Government with access to the Z drive." The judge therefore reversed the magistrate judge's ruling quashing the subpoena, reinstated the subpoena, and ordered Sebastien to provide an unencrypted version of the hard drive. I assume the decision is being appealed to the U.S. Court of Appeals for the Second Circuit. If it is, it could take years for that court to decide the case. If it is not, then Sebastien either decided to produce an unencrypted version of his hard drive, or he is sitting in jail for contempt.

The Boucher case is not about e-mail or real-time Web surfing, but it does deal with our ability to protect digital information from the government. In other words, it deals with the same privacy concerns that prompted the adoption of the Fourth Amendment. If we can use encryption to secure data, e-mail, and other online activity, we can alleviate the effects of the Smith and Jackson rulings. But encryption is effective only if we cannot be forced to give our encryption keys to the government. Under the federal magistrate judge's ruling, we can use encryption to put digital data permanently beyond the government's reach. Under the district court judge's ruling, we can use encryption to protect our data from private citizens but not from the government.

FINAL THOUGHTS

In this chapter, we have dealt with only a few of the many privacy issues that result from our use of computer technology. However, the issues we addressed are representative of the questions that arise in this context. The dominant theme in this area of the law is that we have to make a choice:

Do we want to be able to assume privacy, or are we satisfied with having to invoke privacy?

If I can assume privacy, then I will not need to encrypt my e-mail or take other measures to ensure that the government cannot gain access to what I have created or what I have done online. I can simply assume that the government cannot obtain that information without obtaining a search warrant. Making it easier for us to enjoy privacy will in no way erode the government's ability to obtain information, as long as it complies with the Fourth Amendment. Creating a system in which we can assume privacy brings more information within the scope of the Fourth Amendment, which simply means that the government has to comply with the requirements of the Fourth Amendment to obtain that information.

If we were going to shift from an environment in which we must invoke privacy to one in which we can assume privacy, we would have to decide what standards we would use to distinguish between what is, and is not, constitutionally private. More precisely, we would have to decide what standards we would use to decide what aspects of our online activities are, and are not, private. The standards we have in place for real-world searches and seizures are, for the most part, satisfactory because they are grounded in activity that has changed very little, if at all, in the last 400 years.

The problem we would face in fashioning standards to expand online privacy is the one I noted earlier: portable privacy. Privacy has historically been spatial privacy; enclaves (homes, businesses, locked boxes, sealed letters) were private because they were spatially isolated. We still live parts of our lives in spatially isolated enclaves, but even in those enclaves, we are linked with the external world. Modern communications technology has created a twenty-first-century version of the Olmstead issue.

In the Olmstead case, the Prohibition agents were able to hear what Olmstead was saying inside his home by tapping into wires outside his home and listening to his phone calls. In so doing, they did not violate the spatial privacy of his home by crossing his threshold without a warrant, but they achieved the same thing by using technology. Under the Katz case, law enforcement officers cannot obtain the contents of a phone call without getting a search warrant, but they can obtain a great deal of other information. As we have seen, they can find out who I am calling and who is calling me; who is e-mailing me and who I am e-mailing; and the information I post in publicly accessible areas of the Internet (and, if someone betrays me, the information I post on password-protected sites). They also can track what I do when I am online, the Web sites I visit, how long I stay on a site, what I do there, what I buy at online stores, and so forth. In addition to all of that,

under the Smith decision, the officers can obtain my financial records, my utility records, my mortgage or leasing information, information about my insurance policies, and a host of other data, all without obtaining a search warrant. If I have an alarm system in my home, they can gain access to records that will let them know when I leave and when I return (assuming I arm it when I leave and disarm it when I return).

We have come close to realizing the prediction Justice Brandeis made 80 years ago: "Ways may . . . be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose . . . the most intimate occurrences of the home."[107] Because technology will become more sophisticated and more pervasive, its corrosive effect on privacy will only accelerate unless the Supreme Court revisits the Smith case and some of its other decisions and develops an interpretation of the Fourth Amendment that goes beyond spatial privacy.