THINKING THROUGH SENTENCING IN COMPUTER HACKING CASES: DID THE U.S. SENTENCING COMMISSION GET IT RIGHT?

Richard W. Downing*

The factors courts consider in sentencing traditional criminal violations often do not include all of the appropriate factors that courts should consider in sentencing computer hackers. In particular, certain relevant factors cannot readily be quantified in monetary terms, such as invasions of privacy and risks to critical economic infrastructures. This article discusses the relevant considerations for sentencing in computer hacking cases and evaluates the effectiveness of the 2003 reforms to the U.S. Sentencing Guidelines.

Over the past five years, the prevalence of computer hacking crimes and the significance of their consequences have continued to grow. The conviction of Scott Levine in 2005 marked a milestone in the theft of electronic information: by accessing corporate databases of an Arkansas company without authorization, he and his conspirators copied over one billion records containing personal information.¹ Similarly, the MS Blaster worm caused a new level of economic disruption when

---

* Richard Downing received a B.A. in Political Science from Yale University and a J.D. from Stanford Law School. He is currently Assistant Deputy Chief of the Computer Crime and Intellectual Property Section, United States Department of Justice. The views expressed in this article are those of the author and do not necessarily reflect the positions or opinions of the United States Department of Justice.

it shut down railroad switching computers across the Southeastern United States.\footnote{Jonathan Adams & Fred Gutel, \textit{Bringing Down the Internet}, \textit{Newsweek}, Oct. 28, 2003, available at http://msnbc.msn.com/id/33396387; 'Slammer' Worm Could Pick Up Steam Monday, CNN.com, Jan. 27, 2003, http://www.cnn.com/2003/TECH/internet/01/26/internet.attack/; Press Release, U.S. Dept' of Justice, Louisiana Man Arrested for Releasing 911 Worm to WebTV Users (Feb. 19, 2004), http://www.cybercrime.gov/jeansonneArrest.htm.} The serious harm caused by these attacks on computers and information\footnote{Although the definition of what constitutes “cybercrime” is far from settled, see Richard W. Downing, \textit{Shoring up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Laws to Combat Cybercrime}, \textit{43 Colum. J. Transnat'l L.} 705, 711 (2005); this article will consider those crimes in which the “victim” of the crime is a computer or information stored by a computer. Thus, unauthorized access to a computer, damage to a computer, or threats to damage a computer all fall within this rubric. The United States Code focuses these offenses in title 18, section 1030, although other parts of title 18 contain related offenses. \textit{See, e.g.}, 18 U.S.C. § 2701 (2000) (criminalizing access to or malicious destruction of email). This article will not consider traditional crimes facilitated by computers and the Internet, such as online fraud and the electronic distribution of child pornography.} clearly show the need for the justice system to adequately deter and punish this conduct.

When considering the need for deterrence, it is important to understand the difficulty of successfully catching and punishing hacking offenders. This difficulty arises from a number of factors. First, the victims of computer hacking often do not detect the unauthorized access on their systems, and organizations that do detect hacking often do not report it to law enforcement because of fears of adverse publicity.\footnote{See Computer Security Institute & Federal Bureau of Investigation, 2006 CSI/FBI Computer Crime and Security Survey, July 13, 2006, at XX, http://www.gocii.com/forms/fbi/csi_fbi_survey.jhtml.} Second, once law enforcement opens an investigation, the crime is very hard to investigate. The protocols underlying the Internet were not designed with identification of users as a priority,\footnote{Hearing on the Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age Before the Senate Committee on the Judiciary, 106th Cong. (Sept. 6, 2000) (statement of Vinton G. Cerf).} and criminals can achieve anonymity fairly easily through the use of throw-away email accounts and proxy servers that hide the true source of communications.\footnote{Michael E. O'Neill, \textit{Old Crimes in New Bottles: Sanctioning Cybercrime}, 9
training and equipping law enforcement officers to investigate computer hacking means that for the foreseeable future, there will not be adequate investigative capability. This problem is particularly severe for smaller police agencies in state and local jurisdictions, and for many foreign law enforcement agencies. Thus, the likelihood of punishment for any particular offense remains quite low.

Under one theory of sentencing, the level of deterrence caused by the criminal justice system is the likelihood of apprehension and punishment multiplied by the degree of punishment.\(^7\) In other words, in a world of rational actors with perfect information, as the likelihood of apprehension drops, the level of punishment must increase in order to obtain the same level of deterrence for a particular crime. According to this theory, given the relatively low likelihood of apprehension for cybercrimes, the criminal justice system needs to assure appropriately stiff sentences in order to achieve more effective deterrence.\(^8\)

Commentators, of course, have pointed out that those intent on violating the law do not always act rationally, nor do they necessarily have accurate information about the likelihood of their apprehension and eventual punishment.\(^9\) Nevertheless, cybercrimes by their very nature allow offenders to commit the offenses without leaving their homes and with a veil of anonymity. This lack of contact with the victims of their crimes and insulation from law enforcement may cause them to be  


\(^8\) See O'Neill, *supra* note 6, at 259-64.

\(^9\) See Lucian Ayre Bechuk & Luis Kaplow, *Optimal Sanctions When Individuals Are Imperfectly Informed About the Probability of Apprehension*, 21 J. LEGAL STUD. 365 (1992); Micheal K. Block & Robert C. Lind, *An Economic Analysis of Crimes Punishable by Imprisionment*, 4 J. LEGAL STUD. 479 (1975). One commentator has suggested, however, that computer criminals may be more rational than other criminals in evaluating the costs and benefits of committing a crime because the Internet provides a low-cost way for potential criminals to learn about the law and its sanctions. O'Neill, *supra* note 6, at 268.
under-deterred. Only successful prosecution and significant punishments will supply prospective cyber-criminals with the information needed to create real deterrence.

Congress has recognized the importance of providing tough penalties for network attacks. In 2001 and again in 2002, Congress raised the maximum penalties for certain portions of the Computer Fraud and Abuse Act. In addition, Congress instructed the U.S. Sentencing Commission to reconsider how the U.S. Sentencing Guidelines (hereafter, "USSG") treat computer hacking offenses. This review resulted in revisions in 2003 that improved the way in which the USSG treat such offenses. Yet flaws in these revisions, as well as advances in the technology and the manner in which the offenses are committed, suggest that the USSG need a fresh look.

This article explores the various factors that courts should take into consideration when sentencing computer hacking offenses. Many of the considerations that would normally apply to white collar crime offenses are appropriate here as well. But because many additional harms occur—especially those that

---

10 Both the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (hereinafter “USA PATRIOT Act”), and the Homeland Security Act, Pub. L. No. 107-296 (2002) (hereinafter “Homeland Security Act”), raised the maximum penalty for computer hacking offenses. For example, the USA PATRIOT Act increased the maximum penalty for intentionally damaging a computer from five years imprisonment to ten years. USA PATRIOT Act, § 814. The Homeland Security Act addressed the situation where such offenses cause bodily harm. Under the revised title 18, section 1030(c)(5), a court has the discretion to impose life in prison where death results from intentional damage to a protected computer. Homeland Security Act, § 225(g). Indeed, as recently as 2006, the House Judiciary Committee approved a bill that would again raise the maximum penalties for computer hacking offenses. H.R. 5318, 109th Cong., 2nd Sess., § 8 (2006), available at http://thomas.loc.gov.

11 In 2005, the Supreme Court struck down mandatory application of the USSG. United States v. Booker, 543 U.S. 220 (2005). Despite this ruling, the USSG remain an important guide for sentencing, and courts have continued to apply them in most cases. The Sentencing Commission recently reported that in fiscal year 2006, courts imposed sentences outside of the guidelines only 14.1% of the time (excluding downward departures at the request of the government). United States Sentencing Commission, Special Post-Booker Coding Project, July 6, 2006, at 1, available at http://www.ussc.gov/Blakely/PostBooker_060106.pdf. Because Booker has given federal courts greater discretion, they can apply the factors discussed in this article without waiting for the U.S. Sentencing Commission to amend the USSG.
cannot readily be measured in monetary terms—courts should consider a variety of other factors to avoid inappropriately light sentences. For example, courts must take into account physical harm to individuals, privacy invasions, and the impact on critical economic infrastructures and governmental functions. Only a broad-based consideration of the effects of such crimes will allow for appropriate sentencing, and the Sentencing Commission should revise the USSG to take these factors into account.

MONETARY HARM

Courts have historically looked at the monetary harm suffered by a crime victim when considering the seriousness of a particular offense, particularly where the crime has a financial motivation. For example, when considering the appropriate punishment for insurance fraud or embezzlement, the financial harm to the victim provides a rough approximation of the significance of the offense, and sentencing schemes such as the USSG direct judges to increase the penalty in proportion to the financial harm.\textsuperscript{12}

This theory of sentencing applies equally to hacking crimes, but with some slight adaptations. Certainly, some hacking crimes are completely analogous to traditional white collar crimes. If a hacker breaks into the online banking servers of a financial institution and transfers money into an account he controls, courts should give appropriate weight to the financial harm suffered by the victim just as they would in a real-world bank fraud case.

\textit{Damage to Computers or Information}

Where the goal of the crime is simply to cause damage to the victim computer, however, the economic losses incurred by the victim are certainly relevant but must be evaluated with care. In the case of computer hacking, "damage" does not, of course, usually mean the physical destruction of a tangible thing. Instead, it means an impairment to "the integrity or

\textsuperscript{12} United States Sentencing Guidelines, § 2B1.1(b) [hereinafter U.S.S.G.].
availability" of data or a computer system. This type of damage can be accomplished, for example, by deleting data, by changing information in a database, by crashing a computer, or by simply making it unavailable to users by flooding its network connection with junk information. Very often, this sort of “damage” does not cause any permanent harm to the victim computer. Once the problem is corrected—the computer is repaired or the flood of junk information cut off—the computer can continue to operate as it did prior to the crime. Yet the cost of these repairs can be significant, particularly where the owner needs to hire an outside computer security consultant. Thus, sentencing courts should consider these costs in calculating the economic harm caused by the offense.

Moreover, in some cases the sole goal of the hacking crime is to make a computer unavailable. In one case, the owner of an online satellite television company paid hackers to use a “denial of service attack” to shut down his competitor’s computers for two weeks. When the victim company could not sell its services, it lost profits. In sentencing the offender, a court should take into account this real financial harm.

In addition, some hacking crimes create significant costs in restoring the owner’s confidence in the integrity of data. If a

---

13 See, e.g., 18 U.S.C. § 1030(c)(8).
hacker intrudes into the servers that handle a hospital’s billing, for example, the system administrators may not be able quickly to determine what records the hacker changed. It may take many employees many days to reconstruct the data in order to make sure that they have detected all of the alterations. Courts should consider the cost of restoring the computer owner’s confidence in the data stored on the victim computer when evaluating the significance of the hacker’s crime.

Theft of Information

A slightly different situation occurs, however, where the hacking crime involves the “theft” of information. In general, the value of real-world stolen property is a good measure of the significance of the crime.\(^{16}\) The theft of electronic information, however, differs in one significant respect: the offender generally only copies the data and does not deprive the owner of possession or use of it. While this circumstance will reduce the harm experienced by the victim, the value of the information remains a good proxy for the significance of the offense. By comparison, consider the situation in which a bank detects embezzlement quickly and stops the transfer of funds out of the victim’s account. Like the owner of illegally copied data, the bank account owner is not deprived of the use of his property, but no one would argue that the amount of money in the attempted transfer is irrelevant at sentencing.

Moreover, in the case of computer data, it may prove difficult at times to establish the value of the information. Some types of information, such as a customer list, have a market value that can be established at trial through expert testimony or by introducing evidence that the offender sold it to another

---

\(^{16}\) See 18 U.S.C. § 2314 (creating federal violation for interstate transportation of stolen goods only where stolen goods’ value exceeds $5,000); U.S.S.G., § 2B1.1(b) (2004) (recommended sentence for theft and embezzlement offenses increases in proportion to the loss sustained by the victim). Congress has also used this criterion in setting the maximum penalty for hacking crimes where the offender obtains information from a computer without authorization. 18 U.S.C. § 1030(c)(2)(B)(iii) (where the value of information obtained exceeds $5,000, maximum penalty increases from one year in prison to five years in prison).
person. But it may be impossible to put a price tag on other types of information, even though it plainly cost someone a considerable amount of money to create the data. For example, an individual broke into a NASA computer in 1999 and stole a software program developed to control the physical environment on the International Space Station. It cost NASA $1.7 million dollars to develop this software, but it probably has no value on the open market. Similarly, in 2000 several employees of Lucent Technologies stole the source code to a new server designed to handle voice and electronic data that cost millions of dollars to develop. The offenders intended to transfer the technology to China. Because of business decisions, however, Lucent discontinued its product, and the current market value of the software may be zero. In these situations, the cost of developing the information provides a reasonable alternative measure of its value, and courts should utilize this value in calculating the harm caused by the offense.

Sentencing Guidelines

Amendments to the USSG in 2003 greatly improved the treatment of damage to a computer. Under Section 2B1.1, the USSG define “actual loss” to include the following harms, regardless of whether they were reasonably foreseeable:

17 Of course, the price at which stolen data is sold, sometimes called “black market” price, generally substantially under represents the true value of the information. Buyers of stolen data presumably would not pay full price because of the risk that the data may not be reliable or genuine, and because they risk prosecution for possession of the stolen information.


19 Press Release, supra note 18.


22 Id.
Any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.\textsuperscript{23}

This broad definition, now identical to the statutory definition of "loss" in 18 U.S.C. § 1030(e) provides good coverage for the kinds of economic harms victims experience when their computers are shut down or where offenders impair their data or system security.

This loss definition, however, completely ignores the harm to victims caused by the theft of information. Indeed, by providing a specific definition of loss for offenses under 18 U.S.C. § 1030, it makes it harder for the government to argue that courts should take into account other measures of loss—such as the market value of information—and to counter defendants’ arguments that a court should ignore the value of illegally copied information because the offense did not interfere with the victim’s use of the information. Thus, the U.S. Sentencing Commission should consider broadening the treatment of loss to cover information theft offenses. Moreover, the USSG should explicitly direct judges to take into account the development cost of information as an alternative to the other measures of the value of information, such as market value.

The following language would accomplish this result:

(III) Offenses Under 18 U.S.C. § 1030.—In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages

incurred because of interruption of service.\textsuperscript{24}

In addition, where the offense involves obtaining information, actual loss includes the value of that information, regardless of whether the owner was deprived of its use. If the market value of information is difficult or impossible to determine or does not adequately reflect the significance of the information, the value of the information will be the cost incurred to develop or compile the information.

\textbf{THE INTENT OF THE OFFENDER}

As with many traditional crimes, sentencing courts should consider a computer crime offender’s intent. Where the object of the crime is the theft of information,\textsuperscript{25} fraud,\textsuperscript{26} or extortion,\textsuperscript{27} the definition of the offense already includes a particular mental state. Offenders, of course, seldom \textit{recklessly} extort someone or \textit{negligently} obtain money under false pretenses. Courts should have little difficulty in taking their criminal intent into account.

In the case of damage to a computer, however, the actor could have a variety of mental states. In some cases, the offender has acted intentionally to access a computer without authorization but then inadvertently causes the system to crash. This negligent or reckless damage can have serious consequences—such as when a juvenile shut down the regional airport in Worcester, Massachusetts, in 1996 by breaking into a telephone company computer and accidentally causing the machine to crash\textsuperscript{28}—but the offender should be treated more leniently than if the conduct were fully intentional. By contrast, Jeffery Lee Parson released a worm that not only spread

\textsuperscript{24} 18 U.S.C. § 1030(a)(11).
\textsuperscript{25} See, e.g., 18 U.S.C. § 1030(a)(2).
\textsuperscript{26} See, e.g., 18 U.S.C. § 1030(a)(4).
\textsuperscript{27} See, e.g., 18 U.S.C. § 1030(a)(7).
aggressively and monopolized communications bandwidth, but it caused computers around the world to deluge Microsoft with spurious data that shut down its Internet connection for hours.\textsuperscript{29} Plainly, courts should treat these two offenders differently due to their differing degrees of intent, quite apart from the damage that their acts actually cause.

\textit{Sentencing Guidelines}

Congress created a graduated sentencing scheme for the Computer Fraud and Abuse Act. Unauthorized access to a computer when combined with any amount of damage constitutes a one-year misdemeanor offense,\textsuperscript{29} but that offense rises to a five-year felony where the offender causes the damage \textit{recklessly}.\textsuperscript{31} The statute reserves the ten-year maximum imprisonment for offenders who damage computers \textit{intentionally}.\textsuperscript{32}

Like the statutory maximums created by Congress, the USSG explicitly address the question of intent. If the offender causes damage intentionally, the USSG call for a four-level increase.\textsuperscript{33} Unfortunately, the subsection that contains this increase contains a number of bases for an increased guideline range, and this mix of factors does not always lead to the appropriate outcome. The source of this problem is the subsection’s directive to “Apply the Greatest” of three elements, each of which should be treated separately in most cases. For example, the first of these elements directs the court to increase a defendant’s guideline range by two levels if the offense includes the unauthorized access to a military computer or the theft of personal information. If the offender also intentionally


\textsuperscript{31} 18 U.S.C. § 1030(c).

\textsuperscript{32} Id.

\textsuperscript{33} Id.
causes damage, however, he triggers the second element, a four-level increase, and the court will ignore the first element. Thus, if the offender intentionally damages a computer that controls the power grid, the USSG would assign him the exact same guideline range as someone who intentionally damages a grocery store computer. This outcome makes little sense, and the Sentencing Commission should allow each of these elements to apply independently of one another.

The following wording would accomplish this result:

(14)(A) (Apply the greatest) If the defendant was convicted of an offense under 18 U.S.C. § 1030 and:
   (i) the offense involved a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security increase by TWO levels.
   (ii) the offense caused a substantial disruption of a critical infrastructure, increase by SIX levels. If this level is less than level TWENTY-FOUR, increase to level TWENTY-FOUR.

(B) If the defendant was convicted of an offense
   (i) under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information, increase by TWO levels.
   (ii) under 18 U.S.C. § 1030(a)(5)(A)(i), increase by FOUR levels.

SMALL HARMS TO MANY VICTIMS

In many cases, computer hacking crimes cause harm to thousands or even millions of victims. In many such cases, however, the harm sustained by each individual computer owner may be comparatively slight and difficult to assess. For example, a home user’s computer could become infected by a computer worm that causes the operating system to crash unexpectedly. The computer user may need to spend several hours finding, downloading, and using a software tool to clean up the system, and she might lose data from a document that was open at the time of the computer crash. Likewise, a worm
could copy all address books on the victim computer and send the information out to the worm's author for later use in sending spam. In both these cases, the victim does not suffer any significant financial loss or easily measurable harm. Yet when these small inconveniences or invasions of privacy of thousands of users are added together, the total harm caused by the crime can be considerable.

This common scenario can cause difficulties in the context of a criminal prosecution, however. Prosecutors may find it difficult to present evidence of these small harms at the sentencing phase of a trial. As the government plainly cannot present the testimony of thousands of witnesses or even identify every single person who has suffered harm, courts should allow the government to present the testimony of several representative victims. The government may then be able to call an expert witness to extrapolate from these examples based on the expert's knowledge of the effects of the computer worm. In this way, courts can gain at least a rough assessment of the crime's aggregate harm in many cases.

*Sentencing Guidelines*

The USSG contain an effective approach to address those situations where calculations of the total harm are uncertain or impossible. In addition to increasing the guidelines' range based on harms measured in monetary terms, the USSG direct courts to increase sentences where the crime affects multiple victims.\(^{34}\) Section 2B1.1(2) raises the guidelines' range by two levels where the crime involves more than ten victims, by four levels where it involves more than fifty victims, and by six levels where it involves more than 250 victims.\(^{35}\) This supplemental increase helps to assure an appropriate outcome where

\(^{34}\) *U.S.S.G. § 2B1.1(2).*

\(^{35}\) *Id.* Of course, virtually every crime involving a virus, worm, or botnet will have more than 250 victims, so one could conceive of a special category for these offenses with extremely widespread effects. However, the six-level increase for more than 250 victims probably adequately addresses the need for increased sentences for these offenses.
many victims receive a small financial harm.

Unfortunately, the USSG do not similarly take into account victims who do not suffer financial harm. Application Note 1 restricts the definition of “victim” to include only those who have suffered loss that can be measured in monetary terms. Thus, if the worm invades the privacy of many computer owners but does not cause any quantifiable monetary loss, the increases for multiple victims do not apply. Yet it makes no sense for the guidelines to direct courts to enhance sentences for privacy invasions but then define “victim” to be only those that suffer monetary harm. The Sentencing Commission should address this problem by amending the definition of “victim” so that it includes persons whose privacy was invaded by the criminal offense.

INVASIONS OF PRIVACY

As computers have become increasingly ubiquitous in our society, the amount of personal information stored in digital format continues to multiply. Companies store vast amounts of sensitive information about people, such as medical and financial records. Individuals have also taken advantage of computer resources, storing information such as diaries, personal correspondence, online banking and investing, wills, tax returns, and calendars. As more and more computer networks serve as repositories for private information, computer intrusions now have unprecedented potential to expose the personal information of hundreds or thousands of users at once.

Computer intruders attempt to obtain such information for a wide variety of reasons. For example, in 2000, a group of hackers broke into computers across the United States as part of a scheme to steal credit cards and other identity information and use it to commit fraud. Vasilii Gorshkov was convicted, among other things, of possessing over 50,000 credit card numbers. Hackers have also accessed medical records for finan-

---

cial gain. Several years ago, a hacker accessed a Pittsburgh hospital to obtain the medical records of a popular country western singer in order to later sell them to a tabloid newspaper.\textsuperscript{38} Many information thefts, however, are motivated by curiosity or a prurient interest, rather than a monetary one. Prosecutors recently indicted five people for designing and selling a software program that buyers could use to spy on others, such as their spouses, girlfriends, or ex-lovers. Once surreptitiously installed on a computer, the “Loverspy” program would access stored files and relay them to person who installed it. Many others across the country have been indicted for using “Loverspy.”\textsuperscript{39}

Courts may find it difficult to evaluate and properly sentence this sort of conduct. As discussed above, when an intruder copies digital information, it generally does not prevent the owner from continuing to use that information, and it may be difficult to measure the privacy invasion in monetary terms. In addition, even where the crime has an economic motivation—such as where a hacker steals financial information and uses it to commit fraud—the crime generally causes a significant privacy invasion quite apart from the monetary harm. Indeed, where a bank makes the customer whole, the privacy invasion may be the most salient harm. Moreover, in most cases, if the person who steals the information discloses that information to someone else, the privacy invasion is aggravated. Thus, where a hacker sells identity information on the black market,\textsuperscript{40} or where a spurned lover intercepts private emails and then posts them on the Internet, the severity of the

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{38} Selling Singer's Files Gets Man 6 Months, \textit{Houston Chronicle}, Dec. 2, 2000, at A2.
\item\textsuperscript{40} See, e.g., Press Release, Dept of Justice, Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy — Shadowcrew Organization Was Called ‘One-Stop Online Marketplace For Identity Theft’ (Nov. 17, 2005), available at http://www.cybercrime.gov/mantovaniPlea.htm.
\end{itemize}
\end{footnotesize}
harm increases dramatically.

Sentencing Guidelines

Policymakers considering the drafting of guidelines to address privacy invasions are faced with a difficult task. Plainly, not all information is equally sensitive, and creating rules to take into account varying sensitivities between different types of "private" information can prove elusive. For example, no one expects publicly listed phone numbers to remain private, but if hackers get access to a celebrity's address book the invasion of privacy can be significant. Similarly, a home user's computer may contain thousands of family photographs that the owner does not regard as particularly confidential, but that person would almost certainly feel quite differently if a pedophile were to gain access to pictures of his or her children.

Moreover, individuals have differing sensitivities to the disclosure of their information. Some people may care little about the disclosure of their wills or tax returns, while others would be deeply disturbed to have this information made public. Indeed, some people have a deep-seated concern about the disclosure of even the more mundane aspects of their lives—such as where they choose to shop or how much money they spend on telephone calls.

For this reason, sentencing guidelines should allow a large degree of discretion to the sentencing court to examine the facts of a particular case, evaluate the harm to the particular victims, and fashion an appropriate sentence. Such guidelines can, however, play a role in assuring that sentencing courts do not ignore the various ways in which privacy can be invaded.

The USSG does a credible job of meeting these two goals. On the one hand, the USSG prescribe a two-level increase where the offense involves the intent to obtain "personal information."\(^4\) The definition of "personal information" provides

\(^{41}\) *Paris' Pals Besieged with Calls After Her Cell Phone is Hacked*, Chicago Sun Times, Feb. 23, 2005, at 52 (hackers gained access to celebrity Paris Hilton's cell phone and posted phone numbers from the phone on the Internet).

courts with the following non-exclusive list:

Personal information means sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including e-mail; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.\textsuperscript{43}

Notably, this definition does not require that the personal information be in the possession of the person about whom the information pertains.

On the other hand, the USSG provide broad discretion for courts to increase the penalty where the facts of a particular case demonstrate a “substantial” privacy invasion. They explicitly recommend an upward departure from the guideline range that would otherwise apply where “[t]he offense caused or risked substantial non-monetary harm. For example, the offense . . . resulted in a substantial invasion of a privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records).”\textsuperscript{44}

Thus, for example, where a man obtains unauthorized access to the personal emails of a woman as part of a stalking offense, the USSG would call for a two-level increase for the obtaining of personal information and encourage the court to increase the sentence above the guideline range due to the significant privacy invasion.

The USSG do have one shortcoming: they do not explicitly address the situation in which private information is disclosed beyond the individual who gains unauthorized access to it. Because this act virtually always increases the significance of the privacy invasion, the Sentencing Commission should consider amending the USSG to include an additional two-level increase for such an action.

Building on the changes proposed above, the following amendment would accomplish this result:

\textsuperscript{43} U.S.S.G. § 2B1.1, n.13(A).

\textsuperscript{44} U.S.S.G. § 2B1.1, n.19(A)(ii).
(B) If the defendant was convicted of an offense
(i) under 18 U.S.C. § 1030 and the offense involved an intent
to obtain personal information, increase by TWO levels. If the
offense involved the disclosure of such personal information to
another, increase by an additional TWO levels.

PHYSICAL HARM TO INDIVIDUALS

Although there has been no documented case of a death
caused by unauthorized access to a computer, a number of
close-calls suggest that it is only a matter of time. For example,
in 1997, one hacker recklessly damaged a telecommunications
switch that interrupted service at a regional airport in Massa-
chusetts. For hours, approaching pilots were unable to activate
the runway landing lights, and communications with emer-
gency services were inoperable. 45 A similar risk to life and limb
occurred when Rajib Mitra disrupted police radio service in
Madison, Wisconsin, on Halloween, 2003. Although no physical
injuries were reported, it was in part the threat of such harm
that caused the judge to sentence Mitra to eight years in priso-
on. 46 It is also not difficult to imagine a malicious hacker dis-
rupting service at a hospital with the intent of causing harm to
patients.

Of course, courts routinely sentence for offenses that in-
volve physical injury and death. Courts can readily take into
account the conduct if they examine the offender’s mental state
with respect to the physical injury. For example, if the offender
fully intends to access a hospital computer and alter a patient
database, but is reckless about the possibility that death would
result, then the appropriate penalty should emulate that for

45 Press Release, U.S. Dept of Justice, Juvenile Computer Hacker Cuts off FAA
Tower at Regional Airport—First Federal Charges Brought Against a Juvenile for
hm.

46 Reid J. Epstein, Hacker Convicted in Police Radio Case—He’ll Be Sentenced
May 12 for Transmitting Sexually Explicit Sounds, MILWAUKEE JOURNAL SENTINEL,
Mar. 5, 2004, at B1; Kevin Murphy, 8-Year Sentence for Radio Interference—UW
Grad’s Actions Labeled Terrorism, CAPITAL TIMES, May 13, 2004, at 1B.
reckless homicide. Similarly, if the hacker manipulated a patient’s hospital records with the intent to cause that person to die, then the penalty should be commensurate with first degree murder.

Sentencing Guidelines

The USSG section that relates to hacking offenses, Section 2B1.1, covers a broad range of white collar crimes. As such, death or physical injury rarely results from these offenses, and the section does not address this possibility with much precision. In particular, § 2B1.1(12) requires a mere two-level increase “[i]f the offense involved . . . the conscious or reckless risk of death or serious bodily injury.” 47 Section 2B1.1 has no explicit increase where injury or death actually occurs, however. Instead, the USSG give courts broad discretion to issue sentences above the guideline range where, “for example, in an 18 U.S.C. § 1030 offense involving damage to a protected computer, if, as a result of that offense, death resulted.” 48

This broad discretion seems out of place compared with the precision with which the USSG treats injury and death in other sections. For example, § 2A1.1 through 2A1.4 creates a sensible structure for the various mental states related to homicide, and there is no reason that § 2B1.1 could not directly cross-reference that section. Indeed, this type of cross-reference is used in other parts of the USSG, such as § 2L1.1 (Smuggling, Transporting, or Harboring an Unlawful Alien). Such a cross-reference could also clarify that in applying § 2A1.1-4, courts should assess the offender’s mental state with respect to the death itself. Similarly, § 2B1.1 should be amended to include explicit treatment of offenses that cause physical injury. Section 2L1.1 again provides a suitable model: a two-level increase for offenses that cause bodily injury, a four-level increase for serious bodily injury, and a 6-level increase for

47 U.S.S.G. § 2B1.1(12). This section also provides that if the resulting guideline range is below 14, to raise it to 14, thus assuring a recommended sentence of at least 15 months.
permanent or life-threatening bodily injury." These amendments would provide courts with appropriate direction and harmonize this section with other similar USSG sections.

HARM TO CRITICAL INFRASTRUCTURES

"Critical infrastructures" have been defined as "systems and assets vital to national defense . . . economic security, public health or safety." Such infrastructures include the distribution of electricity, banking and finance, telecommunications, government emergency services, and the water supply. Moreover, in the United States, operation of these infrastructures increasingly relies on computer networks, and much attention has been focused on assuring the continuity of these systems. This attention seems appropriate—a catastrophic failure of the electrical grid in the Northeastern United States and Canada, caused by the accidental failure of a single computer, knocked out power to fifty million people, many of whom lost power for more than a week.

Computer crimes have resulted in severe threats to critical infrastructures, such as when hackers gained unauthorized access to computers that controlled the flows of gas in the distribution pipelines of Gazprom, the largest natural gas company in the world. Russian officials reported that no ill effects occurred. Similarly, in 1998 a hacker reportedly broke into the computer system that runs Arizona’s Roosevelt Dam, attaining complete command of the system controlling its massive floodgates. If the sixty-five billion cubic feet of water restrained by the dam had been released, the consequences could have been disastrous for Mesa and Tempe, Arizona, two com-

49 U.S.S.G. § 2L1.1(b)(6).
50 See, e.g., U.S.S.G. § 2B1.1, n.13(a).
munities on the flood plain below the dam with a combined population totaling nearly one million people.54

Moreover, some cybercrimes have actually caused harm to critical infrastructures. For example, in addition to damaging computers around the world and slowing communications networks, the blaster worm shut down the computers that controlled rail switching in the Southeastern United States, disrupting schedules or forcing trains to move very slowly. More ominously, it also crippled the safety system of a nuclear power plant. Luckily, the nuclear reactor was offline for maintenance at the time, and no harm occurred.55 Plainly, courts will have to consider how to appropriately sentence offenders who threaten or disrupt critical infrastructures.

Some of these types of attacks might cause losses that can be measured in monetary terms, and experts could testify at sentencing hearings about them. For example, if a computer attack shuts down the New York Stock Exchange for two days, it would be possible at least to calculate the profit lost by the stock exchange itself and the expenses required to repair the system. Other loss calculations may be impossible, however. How would one measure in dollar terms the interruption of the water supply or the disruption of government emergency services? Courts will need to find ways to take into account these other non-monetary harms.

Drafting guidelines to take non-monetary harms into account, however, is not easy. Because of the significant possibility of inadvertent harm, for example, it makes sense to increase

54 Barton Gellman, Experts Fear Cyber-attack by Al Qaeda — Computers' Role in Controlling Infrastructure, Combined with Security Gaps and Terrorists' Skills, Prompts Concerns About a Catastrophe, CHICAGO TRIBUNE, July 4, 2002, at 9. U.S.S.G. § 2B1.1, Application Note 19(b). It is worth noting that application Note 19(b), unlike the definition of "critical infrastructure" itself, refers only to "national" economic security and "national" public safety. This change in wording suggests that the Commission intended that courts impose the 6-point increase where the harm to critical infrastructures is local or regional and impose sentences above the standard guidelines range where the harm to the economy or public safety is of national significance.

the penalty for any crime that results in unauthorized access to a computer used to control a critical infrastructure regardless of whether harm results. But in order to apply this increase, should prosecutors have to prove that the offender knew the nature of the victim computer? A good argument can be made that these computers require such stringent protection that the offender should receive higher punishment regardless of intent. In other words, offenders take the risk when they break into another's computers and the burden should be on them to know on whose computer they are trespassing.

Another significant problem in developing guidelines is how to take into account the fact that not all “critical infrastructure computers” have the same significance. For example, every computer that routes traffic on the Internet supports the “telecommunications infrastructure.” Yet many of these computers go offline periodically, and disruption of a single computer will not have any noticeable impact on communications traffic. Sentencing guidelines must have some mechanism for courts to differentiate between the intentional disruption of a minor router and an attack that interrupts the flow of oil in the Alaskan pipeline.

Finally, some harms to critical infrastructures threaten life and limb. Those that create this threat—or that actually cause physical injury or death—should be treated with appropriate severity.

Sentencing Guidelines

The U.S. Sentencing Commission has made a number of important changes to the USSG to take into account computer crimes involving critical infrastructures. For example, the USSG supply a good definition of “critical infrastructure”:

“Critical infrastructure” means systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems,
financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public.\footnote{56 U.S.S.G. § 2B2.3, n.1.}

In addition, the USSG instruct judges to take into account the significance of the harm to the infrastructure itself. If the crime in any way involves a computer used to “maintain or operate” a critical infrastructure, the USSG call for a two-level increase.\footnote{57 U.S.S.G. § 2B1.1(14)(A)(i).} If the offense causes a “substantial disruption” to a critical infrastructure, however, the increase jumps to six levels, with a minimum level of twenty-four.\footnote{58 U.S.S.G. § 2B1.1(14)(A)(ii), (B).} Finally, if harm to the infrastructure is so substantial as to have a “debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters,” the USSG recommend courts impose a sentence above the standard guidelines range.\footnote{59 U.S.S.G. § 2B1.1, n.19(B). It is worth noting that Application Note 19(B), unlike the definition of “critical infrastructure” itself, refers only to “national” economic security and “national” public safety. This change in wording suggests that the Commission intended that courts impose sentences above the standard guidelines range only where the harm to the economy or public safety is of national significance.} Although a six-level increase for substantially disrupting a critical infrastructure may be slightly inadequate, the overall framework is very good.

The USSG does, however, have several flaws in its treatment of offenses that affect critical infrastructures. First, as identified above in Section II of this article, § 2B1.1(14) does not allow for cumulative increases where the crime involves intentional damage to a computer and the offense disrupts a critical infrastructure. This lack of aggregation means that the person who intentionally shuts down a state’s power grid will get the same six-level increase as the person who accidentally does so. In addition, as noted above in Part V of this article, § 2B1.1 does not provide adequate cross references to the sec-
tions governing bodily injury and death.

HARM TO GOVERNMENT FUNCTIONS

Like attacks on critical infrastructures, computer intrusions involving certain government computers often cause harms that cannot be measured in monetary terms. For example, elections increasingly rely on computers, both for the casting and the tallying of votes. Disruption of a computer used to tally votes on an election day may be relatively inexpensive to repair, but it can have a significant impact on the perception of fairness among the voters. How can one place a value on the reliability of an election?

Similarly, computer networks are used in furtherance of the administration of justice—by state, local, and federal law enforcement agencies, by jail and prison agencies, by probation and parole offices, and by local, state, and federal courts. Such networks play a role in ensuring that the justice system performs effectively and efficiently so that dangerous criminals are kept off the streets. In one notable case, a convicted felon hacked into the computer network in San Bernadino County, California, and changed the records to show that charges pending against him were dismissed.60 If criminals can modify their sentences, gain early release, or disrupt the functioning of the courts, it could cause a grave impact on the public’s faith in the fairness of the criminal justice system.

Moreover, attacks on military computers can cause harms far beyond those that can be measured by the cost of cleaning up a damaged computer network. For example, a computer intrusion that discloses troop and equipment locations could gravely harm national security and endanger soldiers on the battlefield. Because of the importance of such government functions and because it is generally impossible to measure these harms solely in terms of repair costs or lost profits, courts should give careful consideration to these factors in sentencing.

offenders.

**Sentencing Guidelines**

The USSG provide for increased penalties for intrusions into some, but not all, government systems. Section 2B1.1(14)(A)(i) provides for a two-level increase for *any* intrusion into “a computer system . . . used by or for a government entity in furtherance of the administration of justice, national defense, or national security.”61 This provision appropriately reflects the gravity of such attacks: offenders should be strongly deterred from such conduct.

The USSG also do a credible job in addressing attacks on justice or national security computers that do in fact result in a disruption of service. Courts should rule that defense and criminal justice computers meet the general definition of “critical infrastructures” (“systems and assets vital to national defense, national security, economic security, public health or safety”62) making their disruption qualify for the sentencing provisions relating to critical infrastructures described above. Defense and criminal justice computers, however, are strangely absent from the definition’s list of examples, and the Sentencing Commission should clarify this oversight.63 As noted above, the USSG also direct courts to impose sentences in excess of the guidelines range when “the disruption to the critical infrastructure(s) is so substantial as to have a debilitating impact on national security, national economic security, national public health or

---

63 The following wording would accomplish this correction:

Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations such as the administration of justice and national security or that provide essential services to the public.
safety.\textsuperscript{64} This provision sensibly gives courts the discretion to fashion quite severe penalties in truly egregious cases.

CONCLUSION

As crimes and offenses continue to change with the advance of technology, courts will increasingly be called upon to fashion sentences for crimes that do not fit the traditional patterns. These crimes remain very difficult to investigate, making it likely that many offenses will go undiscovered and many offenders unpunished.\textsuperscript{65} Where the likelihood of apprehension is low, it becomes all the more important that courts impose appropriately lengthy sentences in order to deter the criminal conduct.

These offenses, however, require consideration of a broad range of factors, some of which may be foreign to judges not familiar with information technology. Prosecutors therefore have the burden to educate courts about the real harms that these crimes cause through the testimony of victims and technology experts. The U.S. Sentencing Commission could ease this task and facilitate improved sentencing in computer crime cases by amending the USSG in the ways detailed in this article.

\textsuperscript{64} U.S.S.G. § 2B1.1, n.19(B).

\textsuperscript{65} See O'Neill, supra note 6, at 261.