The Misery of Mitra: Considering Criminal Punishment for Computer Crimes

By James T. Tsai[1]

Introduction

Rajib Mitra always had an interest in computers; his mother introduced him to amateur radios when he was a child and he lived a stereotypical techno-geek lifestyle: an ex-girlfriend described as being just as interested in computers as her, and another girlfriend he met online.[2] His undergraduate major was computer science and his two years of work after college were in software engineering.[3]

Mitra received a B.S. in computer science from the University of Wisconsin in 2000; he also already had a history of two prior convictions of malicious activity with computers. In 2003, Mitra was now pursuing an MBA at the University's graduate business school in Madison, Wisconsin.[4]

The city uses Smartnet II, a computer-based radio system that coordinates communication between the police, fire and other public safety and emergency agencies for the city. The system creates "talk groups" which allows for coordination between any users of the system. Utilizing twenty channels, the system makes effective use of the full radio spectrum. Between January and August of 2003, the system was rendered unusable with blackouts of availability. These events were occasional and spread out. [5]

The City was able to eventually locate the source of a signal that was causing the blackout. The culprit was Mitra.[6]

Mitra was charged under the recently revised Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030. Showing no remorse, he appealed and spoke before an appellate panel including Judge Easterbrook of the Seventh Circuit. He claimed he had done nothing wrong and that the eight-year sentence imposed on him was not fair.[7]

Was the misery that Mitra was experiencing "fair"? The changes made to the Act that Mitra was charged under were made after the terrorist attacks of Sept. 11, 2001 as amended by the USA PATRIOT Act of 2001[8] and by the Cyber Security Enhancement Act pf 2002.[9] The judges called Mitra a "domestic terrorist,"[10] which seemed to reflect the original rationale for the increases in punishment.

This paper analyzes the policies and philosophy of punishment for computer crimes under the post-Sept. 11th regime. I argue that the judicial discourse represented in Mitra represents a willingness to use the Computer Fraud and Abuse Act to go after

---

[1] Written for Prof. Jonathan Clough's Fall 2005 seminar class, Computers and Crime at the Case Western Reserve University School of Law. Submitted Sept. 30, 2005.
[2] Reid Epstein, *Police radio interference draws 8-year prison term*, Milwaukee Journal Sentinel, May 12, 2004, available at http://www.jsonline.com/news/wauk/may04/228998.asp (last accessed Sept. 29, 2005).
[3] U.S. v. Mitra, 405 F.3d 492, 493 (7th Cir. 2005).
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Epstein, *supra* at note 2.
[8] Pub. L. No. 107-56, §814, 115 Stat, 272.
[9] Pub. L. No. 107-296, §225, 116 Stat. 2135.
[10] Epstein, *supra* at note 2.

defendants that cause trouble with critical infrastructures, the so-called "domestic terrorist." This is manifested in the levels of punishments for such offenses and calls into question whether the traditional theories of punishment are applicable. I argue that as a policy, it makes good sense but the hazy definitions of terrorism may present problems for its success, and instead an approach that takes into consideration the perpetrators may help facilitate a resolution to this problem.

I first give a discussion of the historical background and context to §1030. Next, I discuss the increase in punishment levels in § 1030. I then give a discussion about the pervasiveness of computer-chip technology and apply Mitra. Then, I analyze this in the context of theories of punishment, and discuss and present a solution to this slippery-slope problem.

Background

Computer Fraud and Abuse Act 18 U.S.C.A § 1030(c)

Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984[11] in the face of the rise of crime and computers in the country. Congress had been relying on the old mail and wire-fraud statutes to deal with these new, but increasingly prevalent crimes. But issues relating to sufficiency of interstate commerce pushed Congress to pass the Act to deal specifically with the new breed of crimes.[12]

The original 1984 Act dealt specifically with government computers that had classified defense, foreign relations information, financial institution and consumer reporting agency files.[13] This represented the first time computers were dealt with as either a medium for crime or to facilitate a crime.[14]

Subsequent development of computer crime laws may be categorized into two groups: the first involves further amendments to this 1984 Act; the latter involves the subsequent amendments of existing traditional crimes to include the scope of computers and to adjust punishments as necessary.[15]

The scope of this paper will only consider the former of these two developments. The continuing evolution of the 1984 Act yields a microcosm to study punishment's social and public policies.

The 1984 Act was drastically reformed with the National Information Infrastructure Protection Act of 1996.[16] Subsequent amendments were made in 2001 with the USA PATRIOT ACT, the Cyber Security Act of 2002 and the Computer Software Privacy and Control Act of 2004. Separating out into seven different subsections, the Act of today codifies criminal activity with computers. In Figure 1, the contents of the Act are summarized.

---

[11] Pub. L. No. 98-473, 98 Stat. 2190. Also, codified as 18 U.S.C.A § 1030(c).
[12] Shaw v. Toshiba America Information Systems, Inc., 91 F.Supp.2d 926, 930 (E.D. Tex. 1999).
[13] Ryan P. Wallace, Adam M. Lusthaus, Jong Hwan (Justin) Kim, *Computer Crimes*, 42 Am. Crim. L. Rev, 223, n.35 (2005) (citing sources).
[14] JOEL M. ADROPHY, WHITE COLLAR CRIME § 46:2.
[15] Wallace, *supra* note 5, at 229.
[16] 18 U.S.C.A. § 1030 (as amended by the U.S. PATRIOT Act, 2001,

Figure 1 – Anatomy of 18 U.S.C.A. § 1030.

(a)		Unlawful acts
	(1)	Access, or exceeding authorized access and obtaining of confidential information
	(2)	Access or exceeding authorized access to financial records, government agency, or interstate or foreign communications
	(3)	Access to government computer
	(4)	Accesses or exceeding authorized access to commit fraud
	(5)	Transmission of a malcode[17] to cause damage
	(6)	Defraud traffics
	(7)	Extortion
(b)		Attempt clause for all acts in (a)
(c)		Punishment
(d)		Government enforcement, authority
(e)		Lexicon
(f)		Non-applicability to lawful intelligence
(g)		Civil actions

We are most interested in subsection (c), which sets out punishment guidelines. Before we examine this though, let us consider an early case and the resulting punishment from the early version of the Act.

An Early Case: U.S. v. Morris(1988)

The earliest case regarding computers and crime is perhaps U.S. v. Morris.[18] It is apparent from the word usage itself that technology was still quite novel to the courts. For instance, consider Judge Jon Newman's writing of the facts: "Morris released into INTERNET, a national computer network, a computer program known as a "worm" that spread and multiplied, eventually causing computers at various educational institutions and military sites to "crash" or cease functioning."[19]

The complete capitalization of the word INTERNET alone is enough to suggest the novelty of the technology to the court in 1990 when the case was argued. The further definition of "crash" points to the stretching of the bounds of the lexicon of crimes.

Morris was a first-year graduate student at Cornell University's computer science program. As a student in October 1988, he began work on the piece of malcode that would eventually be deployed into the Internet. His goal was to show the chinks in the Internet's security system by reproducing itself and installing itself on machines throughout the Internet.[20] Numerous machines were affected, as much as 10 percent of the Internet at that time, resulting in damage between then-estimated $100,000 and $10

[17] "Malcode" is short for malicious code – it includes various forms of software being sent on the network or directly onto computers. Viruses, worms and Trojans are some of the more familiar terms used. Prof. David Evans advocates the general term malcode to encompass these.
[18] U.S. v. Morris, 928 F.2d 504 (2nd Cir. 1991).
[19] *Id* at 505.
[20] *Id.* at 505-6.

million.[21] Again, this represents the new difficulty in placing damages on this new phenomenon of computer outages.

Morris was found guilty by a jury trial for violating 18 U.S.C. § 1030(a)(5)(A). His sentence was three years of probation, 400 hours of community service and a monetary fine of $10,050 plus the costs of his supervision.[22] The court noted that Morris tried to mitigate the problem by sending out a message over the Internet on how to fix the problem. The network was swamped however and it was simply too late.[23]

The Morris worm, as the literature now calls the malcode, prompted the Defense Adavanced Research Programs Agency (DARPA) to create the Computer Emergency Response Team, which today is a first-line mechanism to deal with malcode attacks.[24]

Incidentally, Morris is an assistant professor today at the Massachusetts Institute of Technology.[25]

Increased punishment

Figure 2 below denotes the structure of punishment for an offense under § 1030. Contrast that with the 1990 version of the same subsection in Figure 3.

[21] United States General Accounting Office, "Computer Security", GAO/IMTEC-89-57, June 1989, available at http://www.ibiblio.org/pub/docs/security/gao-report . This is interestingly the first GAO report made available in electronic format. The header of the report requests feedback on this means for delivering the report.
[22] Morris at 506.
[23] *Id*.
[24] http://www.cert.org/meet_cert/meetcertcc.html
[25] You may visit his website at http://pdos.csail.mit.edu/~rtm .

Figure 2 -- §1030 (c), current through Sept 9, 2005[26]

(c)		Punishment
(1)		(a)(1) offense
	(A)	Fine and/or imprisonment of no more than ten years, first time § 1030 offender.
	(B)	Fine and/or imprisonment of no more than twenty years, repeat §1030 offender.
(2)		(a)(2), (a)(3), (a)(5)(A)(iii) and (a)(6) offenses
	(A)	Fine and/or imprisonment of no more than one year, first time § 1030 offender.
	(B)	(a)(2) offense only – fine and/or imprisonment of no more than five years for (i) offense was for commercial or financial gain; (ii) furthered any criminal or tortious act; (iii) value of the information obtained exceeds $5,000
	(C)	For (a)(2), (a)(3), or (a)(6) – fine and/or imprisonment of no more than ten years for §1030 repeat offender.
(3)		(a)(4), (a)(7), (a)(5)(A)(iii)
	(A)	For (a)(4), (a)(7)– fine and/or imprisonment of no more than five years for first time § 1030 offender.
	(B)	Fine and/or imprisonment of no more than ten years, repeat §1030 offender.
(4)		(a)(5)(a)(i), (a)(5)(a)(ii) (except as provided by ¶5)
	(A)	(a)(5)(a)(i) -- Fine and/or imprisonment of no more than ten years.
	(B)	(a)(5)(a)(ii) -- Fine and/or imprisonment of no more than five years.
	(C)	Fine and/or imprisonment of no more than twenty years, repeat §1030 offender.
(5)		(a)(5)(A)(i)
	(A)	Knowingly or recklessly causes serious bodily injury -- Fine and/or imprisonment of no more than twenty years.
	(B)	Knowingly or recklessly causes death -- Fine and/or imprisonment of any years or for life.

[26] Current through PL 109-63 (excluding P.L. 109-58, 109-59).

Figure 3 -- §1030 (c), USCA 1990 edition

(c)		Punishment
(1)		(a)(1) offense
	(A)	Fine and/or imprisonment of no more than ten years, first time § 1030 offender.
	(B)	Fine and/or imprisonment of no more than twenty years, repeat §1030 offender.
(2)		(a)(2), (a)(3), (a)(6) offenses
	(A)	Fine and/or imprisonment of no more than one year, first time §1030 offender.
	(B)	Fine and/or imprisonment of no more than ten years repeat §1030 offender.
(3)		(a)(4), (a)(5)
	(A)	Fine and/or imprisonment of no more than five years for first time § 1030 offender.
	(B)	Fine and/or imprisonment of no more than ten years, repeat §1030 offender.

Mitra and Morris both perpetrated different crimes and expressed different sentiments about their guilt. Mitra denied to the very end he had done anything wrong and Morris was contrite and showed his good-faith nature in his attempts to mitigate the harm he had caused.

The disparity in sentences is startling as is the contrast in the punishment paragraph of §1030. On first glance, the 1990 version is noticeably simpler and cleaner. The additions in the current version, after only 15 years reflect the added clauses of punishable crimes of §1030(a),(b).

In June 1996, the U.S. Sentencing Commission concluded a report surveying sixty cases between 1988 and 1996. They reported that,

> Federal "computer crime" cases sentenced under the pertinent provisions of 18 U.S.C. § 1030 are relatively uncommon at present. An estimated 60 defendants have been successfully prosecuted and sentenced thereunder in the almost nine years since the guidelines came into existence…. Computer crime defendants receive downward departures from guideline ranges more frequently than do other 'white collar' defendants or federal defendants generally.[27]

[27] United States Sentencing Commission, *Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses*, 2 (1996), available at http://www.usscs.gov/r_congress/COMFRD.PDF (last accessed Sept 30, 2005).

Despite these findings, the Commission still did not make a recommendation for a change in punishment schemes. They wrote, "The limited empirical data available to the Commission and other factors preclude a definite assessment of the deterrent effect of existing guidelines for computer fraud and computer vandalism."[28]

In 2003, after the Homeland Security Act of 2002[29] was passed, the Commission issued a report evaluating the increased penalties that had been put into place for cyber security offenses.[30] It was the first computer crime report the Commission had issued since its 1996 report and it made a single recommendation this time – they recommended increasing statutory maximum penalties for §1030(a)(1) violations, which relate to accessing of national security information.[31] Their rationale was related to the terrorism penalty enhancements for certain crimes from the USA PATRIOT Act, which were above the maximums proscribed in §1030(c).[32]

Congress has not passed any act to date regarding this recommendation to date.

Theories of Punishment

The classical division of theories of punishments seeks to represent the range of reasons why we seek to punish members of our society. Philosophically, there are two main camps for punishment: utilitarianism and retributivism.[33]

Retributivism deals with an idea of just-desserts. People who commit crimes should answer to their actions. This is a backward looking approach that considers the past actions and seeks to justify the punishment solely on the crime that was committed.[34]

Utilitarianism on the other hand seeks to please overall society. Based on Jeremy Bentham's writing human being's nature as creatures of pain and pleasure will affect their actions in their deciding to commit a crime necessarily. In a sense, this is a forward-looking approach; potential criminals will consider the consequences of their actions on themselves.[35]

The Sentencing Commission most likely reflects this latter approach. It mentions ideas of deterring potential offenders by increasing the punishment levels.

Though the reports to Congress seem to suggest only this area of reasoning, the Commission and other members of the legal community have struggled with determining sentencing guidelines. In October 2000, the Commission held a national symposium on Federal Sentencing Policy for Economic Crimes and New Technology Offenses in Arlington, Virginia, outside of the nation's capital. The symposium considered a wide range of issues in addition to computer crimes.

---

[28] *Id* at 9.
[29] P.L. 107-296. The Act required under § 225(c) that the Commission, "submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code."
[30] United States Sentencing Commission, *Increased Penalties for Cyber Security Offenses* (2003), available at http://www.ussc.gov/r_congress/cybercrime503.pdf (last accessed Sept 30, 2005).
[31] *See id*. at 13.
[32] *Id*.
[33] JOSHUA DRESSLER, UNDERSTANDING CRIMINAL LAW 13 (3d ed. 2001).
[34] *Id*. at 16.
[35] *See id.* at 14-15.

One panel had a vibrant exchange on the issue of approaches to punishment beyond deterrence. Judge J. Phil Gilbert responded to a question about deterring effects from sentencing guidelines:

> The deterrence? I have always advocated to our U.S. Attorney, why don't you get billboards and go into these areas where there are high amounts of drug offenses and just put up what the guidelines are? You know, the deterrence is what the press reports people are sentenced to; people read about what someone was sentenced to in a fraud case or theft case. You don't have the guidelines distributed like phone books. I have people appear before me and ask them, "Well, did you know what the guidelines were before you committed this offense?" They say," Heck, no." They didn't even know about guidelines. … You can't limit it to just deterrence. You have got to talk about just punishment and proportionality and you have got to look at the whole picture. You just can't pick one item out. [36]

This conversation seems to be absent from the reports of the Commission however. The latest – and only -- recommendations of the Commission seem to deal with deterring terrorist and critical infrastructure problems.

There are other theories of punishment however. For instance, modern utilitarianism has the notion of rehabilitation – making the punishment try to "fix" the criminal. There is also the idea of denunciation. A good example of this is the scarlet letter that is affixed to the bosom of Hester Prynne, an adulteress in Puritanical America.[37]

As applied to the context of §1030 crimes however, these two theories may still be considered, though their appropriateness as the old saying, "make the punishment fit the crime," would be in question.

A Slippery Slope

Now that the groundwork regarding the background of §1030 and theories of punishment has been set, the question turns to the appropriateness and the implications of the punishment for the offenses.

The Sentencing Commission has made recommendations for penalties only along the vein of deterring terrorist or critical infrastructure claims. Combining this with a plain reading of Mitra however, I argue that a slippery slope ensues to crimes in general.

Mitra argues that a close reading of the statute would have found him to be guilty, but Congress could not have meant it to work in that way. There was no stealing of financial information, or crashing computers; instead, "all he did was gum up a radio system."[38] The theory that Mitra is being held on deals with the fact that there is a computer chip in the hardware of the radio system. This would include just bout every electronic gadget in the world.[39]

---

[36] "The Nature and Severity of Punishment for Economic Crimes; Determinants of Offense Seriousness and Offender Culpability", Symposium on Federal Sentencing Policy for Economic Crimes and New Technology Offenses (2000), 68.

[37] Nathaniel Hathonre, *The Scarlet Letter.*

[38] Mitra at 495.

[39] *Id*. Specifically, "[e]very cell phone and cell tower is a "computer under this statute's definition; so is every iPod, every wireless base station in in the corner coffee shop, and many another gadget."

The court responds that of course Congress could "not contemplate or intend this particular application of the statute." But, the increasing complexity of technology in society today is an impetus for the need to write general statutes since they cannot and most likely aren't complete experts on the fields of technology.[40]

The implication from this is that anyone that commits a crime under this now lower threshold for criminality would suffer the higher levels of punishment. Ostensibly, though this was not argued in the opinion of the case, a question of what is terrorism, especially this new brand of "domestic terrorism,"[41] the threshold to be found a domestic terrorist is also lower.

The public policy results from this are dangerous; the original purpose to punish to deter society occurs, but at the cost of civil liberties to society. Administrative ease to prosecute anyone for almost anything seems to be on the horizon. Is there a way to balance the needs to protect society by having good punishment schemes and also to allow only the appropriate level of punishment for wrongdoers still?

Towards a Solution: Considering Internal and External Perspectives

The Mitra court was correct in its assessment of the rate of technology change and increasing complexity in society today. However, it stops short of asking what the role of the judge and jury is in assessing whether or not the statute extends to the situation at hand. The perspective that the court took was one of an external perspective.

Prof. Orin Kerr has developed the notion of external and internal perspectives regarding how we apply the law to the Internet. "[W]e must first decide whether to apply the law to the facts as seen from the viewpoint of physical reality or virtual reality."[42] Kerr goes on to propose a framework that tries to resolve the problem. The most salient point for the purposes of this paper is to follow the perspective of the person the law seeks to regulate. In this scheme, a conflicting usage of perspectives; one external by the law enforcement, and the other internal by the alleged perpetrator is mediated by balancing the two perspectives in a sort of totality of the circumstances consideration.[43]

Admittedly Kerr's model deals with the Internet and cyber-crimes; Mitra deals with a radio system that had computer chips in it. But are the two really that far apart? The Internet is a specific instance of a network of computers. The radio system in this case, which uses the public airways and regulated by the FCC, as the court pointed out[44] is a "virtual world" in a sense also.

Mitra's obstinacy in that he did not do anything serious can be interpreted as his thinking of just playing games and not really causing anything seriously wrong. To be called a terrorist, which is an external perspective seemed tantamount to a completely disorienting situation.

If we were to consider Kerr's point to follow the internal perspective of Mitra, would we reach a different result? Perhaps not. A reasonable "geek" would still know

---

[40] *Id.*

[41] 22 U.S.C. §2656f(d), is used by the CIA to define terrorism. Under this statute however, there is no mention of domestic terrorism, and as applied here Mitra would not be engaging in terrorism. *See* Neil J. Smelser and Faith Mitchell, "Terrorism: Perspectives from the Behavioral and Social Sciences," NAS/NRC (2002) available at http://books.nap.edu/catalog/10570.html .

[42] Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 357 (2003).

[43] *See Id.* at 400.

[44] Mitra at 496.

about the seriousness of playing with critical infrastructure for his city. But, it would at least provide some mitigation if Mitra were Morris – someone experimenting to try to figure out the chinks in the armor of the system, so to speak.

Consequently, the Commission has its approach wrong; by increasing the maximum penalties, it is not truly deterring the population from these potentially problematic acts; it also may target the Morris' who are trying to contribute something positive to society. If an internal perspective is applied by the courts then that wl lead to appropriate decisions of punishment.

Conclusion

The challenges presented by high innovating societies, and a different set of crimes that are considered because of the emergence of computers presents difficult considerations for how society should treat and punish these new crimes. Liberty and freedom of society cannot be compromised wholesale however in the name of administrative ease and the present-division between the technologically savvy and not will narrow over time, but draconian laws must never be allowed to take root.