GOOD COMPUTING: A VIRTUE APPROACH TO COMPUTER ETHICS

A book under contract with
Jones & Bartlett Publishers
40 Tall Pine Drive
Sudbury, MA 01776
http://www.jbpub.com/

DRAFT FOR
June Puerto Rico writing retreat

Chapter 7
Privacy: Machado
Version 1: 03/03/05 by Chuck Huff

Based on writings in www.computingcases.org prepared by Chuck Huff and Bill Frey and class documents from University of Mayaguez, PR, FILO 3185 prepared by Bill Frey

Table of Contents

Abstract

In September of 1996, 19 year-old Richard Machado sent email to 59 Asian students at his public college, threatening them with phrases like "I will personally make it my life's career to hunt you down and kill you" and signed by "Asian Hater." Several of these individuals reported this incident to the Office of Academic Computing (OAC). One of the recipients was a student employee of the OAC. The administrators of the OAC were faced with a decision about how to respond to harassing and threatening email sent over their system to students of their University, using their facilities. Machado was eventually indicted on federal charges, and convicted of infringing on the civil rights of several of the students who received his email. He served a little over a year in jail for his offense.

Historical Narrative

Richard Machado, at age19, was the first individual to be convicted of a federal electronic mail (email) hate crime. Much attention is currently being drawn to the social and ethical implications surrounding email and Internet usage. The Machado case is one example of a handful of similar incidents that have occurred since the advent of the Internet.

On September 20th, 1996, Machado sent a threatening hate message to 59 Asian students at UCI (University of California at Irvine), via email. The "To:" field in the following email has been omitted in order to protect the privacy of individual recipients. You can see the two versions of the email message with all its SMTP headers (but not recipients) in the historical documents section.

Machado did not receive any immediate response to the email, so he sent it again within a few minutes. Recipients of the email were alarmed by its content. Several students emailed the OAC (Office of Academic Computing, formerly–now the NACS, or Networking and Academic Computing Services) on campus, alerting staff to the incident. The Associate Director of the OAC, with the assistance of student employees, was able to identify Machado as the sender. They traced the computer from which the emails were being sent, and found Machado at that particular computer in the computing lab. Machado was asked to leave. Surveillance cameras in the computer lab later confirmed that Machado was in fact the person responsible for the two threatening email messages.

Following the incident, Machado was reported to the University of California, Irvine Police Department, and an officer was assigned to the case on September 24th, 1996. On September 28th, the officer telephoned Machado's residence, and left a message after he was told that Machado was not home. Machado returned the officer's call later that day, and the two agreed to meet at 5 p.m. When asked about the emails, Machado reported sending them out of "frustration", because the predominance of Asians on campus made it less popular, because Asians raised the grading curve, and because he disliked his Asian roommate. Machado said he felt that Asians "prospered" more in school, and that he just wanted to scare them a little--he never intended actual physical harm. Following the meeting, Machado was charged with "knowingly and without permission using computer services." Machado's trial was set for November 25th, 1996. Machado then agreed to participate in several public forums in which he apologized for his action. He attended these forums and did, in fact, apologize at them.

A few days later, Richard Machado received a call from his brother, asking about an article in the local paper in which Machado was identified as being responsible for an email hate crime. Machado denied his involvement, claiming that the perpetrator must have been someone else with a similar name. Shortly thereafter, Machado disappeared. On November 14th, 1996, a stolen vehicle report was filed at the Police Department for the City of Irvine. The report described Machado as having taken his roommate's car without asking. Machado had allegedly told one roommate that he was borrowing the other roommate's car, and that the other roommate had approved this. The roommate had not in fact given permission, nor had he been aware that Machado was using the car.

On November 18th, 1996, the FBI joined in aiding the investigation of the stolen car. An FBI agent appointed to the case went to Machado's residence and was told by roommates that Machado had not been seen since he had left with his roommate's car keys on the 14th. Machado had lived at this residence since October 1st, 1996. In that time, Machado had also been suspected of other incidents: 1) $80 was missing from a third roommate's coin jar; 2) $154 Visa charges had been made to the roommate's card, of which $54 were unauthorized phone calls on November 10th, 11th and 12th, 1996. Between November 21st and 23rd, 1996, the FBI investigated the case by interviewing the second roommate and Tammy Machado, Richard Machado's sister-in-law. Tammy was told that if Richard did not appear for his court date on November 25th, 1996, a warrant for his arrest would be issued. She said that if anyone in the family hears from Richard, they would encourage him to show up for court.

Machado did not appear at the November 25th court date. A warrant was issued for his arrest, but the investigation could not proceed in his absence. Finally, on February 6th, 1997, Richard Machado was arrested. A United States Immigrations Inspector caught Machado attempting to cross the border at Nogalas, Arizona back into the U.S. from Mexico, where Machado had allegedly been looking for construction work. He later testified in court that he had fled to Mexico after hearing that he could receive 10 years in prison for sending the email messages. A United States Customs Inspector was also present. Machado was reported appearing homeless and without any possessions. Following the arrest, a new trial date was set for September 16th , 1997. Machado was charged with 10 counts of violating the Federally Protected Activities Act of 1968 that makes it a crime to use race, ethnicity or nationality to interfere with a federally protected activity (in this case, students attending a public university).

On November 11th, 1997, Machado’s actual trial began, but a recess was granted when new information was uncovered; the court had been presented with questionnaires that had been given to the victims of Machado’s email, in which 9 of the students said that they had not been overtly bothered by the email. Thus, the trial was delayed until the following Wednesday, November 18th. However, the jury was deadlocked on this day, 9 to 3 in favor of acquittal. A mistrial was declared. A second trial was set for January 27th, 1998, when the case was declared to have national importance by federal prosecutors. A conviction could lead to establishment of legal standards for conduct on the Internet. If it were successful, it would be the first time a conviction was obtained for a person committing an email hate crime under federal hate crime laws.

Throughout the trial, various pieces of information concerning Machado’s background emerged as useful evidence. In the fall of 1995, Machado had sent an email threat to the New University newspaper at UCI using his roommate’s computer. Although Machado was traced to be the sender, his roommate allegedly took the blame. Throughout the following year leading up to his second email hate crime, Machado experienced some personal problems. His eldest brother was killed in an armed robbery. His grades were failing as a result of his difficulty dealing with the death, and Machado was dismissed from school. He continued to tell his parents that he was still a student for three months,

though, because he was the first child in his family to attend college and felt pressure to do well.

The defense in the trial portrayed Machado as a troubled and bored student who was simply trying to gain attention by his behavior. Machado's email looked a great deal like what are called "flames" in the Internet community (much profanity, lots of capital letters), and are usually taken as irritating and impolite, but not illegal behavior. The prosecution pointed out the direct threats of death; the fact that the email was not sent to a mailing list, but to a group of individuals with Asian names, individually identified; to Machado's history of sending email death threats; and to the impact of the threats on the lives of some of the recipients. The defense pointed out that only 10 of the 49 people took the threat seriously enough to want to press charges. Several of the recipients had stated, in response to a police questionnaire, that Machado has a "right to his opinion" and that the email was "no big deal" to them.

On February 13th, 1998, just 3 weeks from the start of the second trial, Machado was found guilty on 2 counts of civil rights violations. Following his conviction, Machado was released on a $10,000 bond from custody, but was soon turned over to Irvine police on pending auto theft charges. Machado's sentencing was postponed until April 10th, 1998. He was sentenced to serve1 year in prison. Machado had already spent 1 year in jail awaiting his trials, and so was free to go. Machado was placed on probation, fined $1,000, required to attend anger and racial tolerance counseling, was not allowed on the UCI campus, was to have no contact with the victims, and was banned from computer usage on the UCI campus. He later violated his probation, and was sentenced to spend four months in a federal halfway house. At last report, Machado was living in Long Beach CA (a neighboring community) with his mother and working for a temporary employment agency.

Time Line

11/16/1995	• Machado sends email threat to New University paper (U of CA,Irvine) via his roommate's computer • the email is traced to roommate's computer, roommate later said Machado had access to the computer • Machado identified as sender
11/21/1995	• Warrant for arrest is filed against Machado, issued by Irvine Police Department--the warrant is a "no bail felony warrant" • Machado consents to a property search • Case given up shortly after --> Machado's roommate took the blame so he "wouldn't be bothered anymore."
(Between 1/1/1996 and 9/20/1996)	• Machado's older brother murdered in armed robbery prior to following incident; • Machado is doing poorly in school, getting pressure from family to uphold high expectations
9/20/1996 (Friday)	• 10:54 am: Machado sends hate Asians/threat email to about 59 UCI students • 11:14 am: Machado sent message a second time shortly after, when he did not receive replies to the first email • incident brought to the attention of Assoc. Director of the Academic Computing Center, Dana Rood, by his employees • Machado identified in computer lab, asked to leave by Core Services mgr.
9/21/1996 (Saturday)	• Director of OAC, Alan Schaino reads Machado’s email and decides that it is a police matter.
9/24/1996 (Monday)	• the incident is reported to University Police Department • An officer is assigned to the case
9/26/1996	• retrieval of surveillance video confirmed Machado as sender • Irvine City Police notified and involved in case
9/27/1996	• registrars office helps police locate Machado's address and

	phone number

9/28/1996	• an officer phones Machado's residence and leaves message
	• Machado calls back and agrees to meet with an officer that afternoon at 5pm
	• charges filed after meeting:
	  ○ --Knowingly & Without Permission Uses Computer Services
	  ○ --Telephone Calls w/ Intent to Annoy

11/14/1996	• a stolen vehicle report is filed for Machado's second roommate's car • Machado had told one roommate he was borrowing his other roommate's car • Machado did not have permission to borrow car
11/18/1996	• FBI attempts investigation • an agent goes to Machado's residence, Machado is not there, and hadn't been seen there since 11/13 • Machado allegedly left with Young's keys on 11/14 • other suspicions: $80 missing from roommate's coin jar; $154 visa charges to roommate's card, $54 of which were unauthorized; calls on 11/10, 11, and 12
11/21/1996	• FBI agent phones Machado's roommate for confirmation of stolen car/info on Machado's disappearance
11/22/1996	• roommate is interviewed
11/23/1996	• Tammy Machado (Machado's sister) interviewed and said Machado disappeared on day his brother called him to inquire about Machado's name appearing in newspaper regarding Asian hate emails. • Machado denied the reports in the paper to his brother; claimed it to be someone else • Tammy is informed that court date is set for 11/25 and if Richard doesn't show, would be warrant for arrest
2/6/1997	• Machado is arrested: was attempting to enter US from Mexico --caught by U.S. Immigration Inspector

	• Machado is reported as looking homeless, having no possessions, looking for construction work in Mexico
9/16/1997	• Machado is charged with 10 counts of inferring with a federally protected activity–in this case, students attending a university • Machado is told he will face up to 10 years if convicted
11/12/1997	• trial takes place, and on this date, a recess is granted when new information is uncovered/presented • questionnaires were revealed in which 9 of the students who got the messages said they were not overtly bothered by Machado's email
11/18/1997	• jury deadlocked, 9 to 3 in favor of acquittal • Case said to have national importance by federal prosecutors, so a second trial was set for Jan. 27, 1998
2/13/191998	• Richard Machado is found guilty on 2 counts of civil rights violations • Took only 3 weeks of trial to reach verdict • Following conviction, Machado is released on a $10,000 bond from custody but is turned over to Irvine police on impending auto theft charges • Sentencing is postponed until April 10, 1998 • Possible maximum time Machado could serve would be 1 yr. • Machado has already spent 1 yr. in jail awaiting trials, so is released. • Machado is recommended for anger & racial tolerance counseling, not allowed on UCI campus, no contact with victims.

Perspective Pieces

Some background on Richard Machado

Richard Machado was born in El Salvador. When his parents moved to California, he went through the required process to become a naturalized citizen of the US. His parents were hard workers and pushed him to succeed in college. He was the first person in his family to attend a college--his other three brothers worked at regular blue collar jobs.

Machado found the academic work at the University of California, Irvine (UCI), to be more difficult than he had expected. He was failing in several of his classes, and he felt that part of the problem was that many Asian students had entered UCI and raised the grading curve too high for him to succeed

On November 16 of 1995, Machado sent an e-mail threat to the campus newspaper at UCI (the New University Paper) using his roommate's computer. The e-mail said "On Monday, November 20, All new u people will die." The editors and most of the staff at the newspaper were Asian. When the e-mail was traced back to the computer, Machado's roommate told the campus police that he sent the message as a joke. He thought that by doing this, the police would be satisfied and would no longer bother them. The investigation was dropped at that time.

That spring, Machado's eldest brother was murdered by an armed robber. This had a devastating effect on him, and he was severely depressed. As a result, his grades dropped even lower and he was dismissed from school in June for academic failure. But he was too ashamed to tell his parents. All that summer, he continued to get rides to the university from a brother, and pretended to be attending classes.

It was the week before the Fall term actually started that Machado walked into the computer lab and composed and sent his e-mail threatening Asians.

Machado and his Email

About 10:30 AM on September 20, 1996, Richard Machado entered EG1122 And sat down at one of the Macintosh computers (labmac3) in this public access computing lab. The University of California, Irvine system requires students to log into the lab machines in order to use certain services. Machado logged into labmac3 at 10:26 AM, using his user ID.

Using the settings in Netscape Mail, he changed the contents of the "From:" field from his actual user ID, Richard Machado <rmachado>, to "Mother Fucker (Hates Asians)" <mfucker@uci.edu>. He sent two test messages to himself to determine if the change in the "From:" field actually worked. It did.

He then used the finger command to list all the people who were logged into the system at that time. From the long list of people logged in he selected 59 individuals, all of whom had one thing in common-- they had Asian looking names. He placed all these user IDs into the "To:" field of a message in Netscape Mail. He also included himself in the To: field.

He composed a message threatening Asian students on campus, and sent it at 10:54 AM. At 10:56 he logged out and left the room.

At 10:57 AM he walked into computer lab room EG1140. He sat down at one computer and could not manage to log in. After failing to log in, he left the room. About ten minutes later, he reentered the same computer lab room and sat down at another computer (pmac13). He checked his messages to see if his earlier message had created any email traffic among those who received it (remember that he listed himself in the "To;" field along with the other people). Since he saw no reaction, he decided to send the message again. He did this at 11:14.

He then proceeded to read his email and use his web browser for about half an hour. Responses to the email were coming in. He composed several replies to these responses, posing as a person who had been targeted by the mail. At that time (11:45), two people from the Office of Academic Computing entered the room and asked him for ID and a telephone number. They said he had been found to be violating school policy. Richard claimed he was not, showed them his student ID and gave them a fake telephone number.

At 11:47 Richard Machado left EG1140 without making any further protest.

When he was later asked about his reason for sending the email, Machado reported sending it out of "frustration," and because he disliked his Asian roommate. Machado said he felt that Asians "prospered" more in school and that they raised the grading curve so far he could not do well. He claimed he just wanted to scare them a little with his email, and get some response.

The University of California at Irvine

The Machado case took place at the University of California at Irvine (UCI), located in Orange County, California. This document provides some background information on the University itself and on race relations on campus and in Orange County.

The UCI admissions web page states the following:

> UCI has been ranked prominently along with much older universities for excellence in the arts and humanities, earth system science, management, social sciences, technology, and information systems. For quality of educational experience and caliber of faculty, UCI consistently ranks among the nation's 10 best public universities, and among the top 50 universities overall. Election to the American Association of Universities (AAU), a group of 60 of the most distinguished research institutions, is another indication of UCI's stature in the academic community.

UCI is a young university, founded in 1964, with its first graduating class in 1968. It has nevertheless achieved distinction as an excellent public university. Admissions standards are competitive, with the average high school GPA being 3.7 and median SAT scores (verbal + math) about 1100.

Orange County
Orange County, California is part of the metro area that makes up the greater Los Angeles area. It is on the southern edge of Los Angeles, and is host to the University of California, Irvine. It is a multi-ethic society, and citizens expect that dealing with race relations will be with them for some time. The following figures are taken from the 1996 Orange County Annual Survey, done by the Department of Urban and Regional Planning at the University of California, Irvine.

- Most people felt the economy was in good shape and that jobs were easy to find
- Crime and immigration were rated as the top two problems people felt needed attention
- 52% of whites reporting voting 4 or more times over the last four years, while only 15% of Hispanics and 6% of Asians reported this much political involvement.

Race and College Representation in California, Orange County, and UCI
Over the past decade, "minority" races have become the majority in California. This is true for Orange County and the University of California, Irvine as well. The table below shows the percentages of the total population that are accounted for by each of several racial groups, using categories from the 1990 census report. Note that though the percentage of Hispanics in the population has been increasing rapidly, their representation at UC, Irvine has remained relatively steady.

	Year	Black	Native American	Asian	Hispanic	Total
California	1990	8%	1%	10%	26%	44%
	1996	8%	1%	12%	30%	50%
	1999	8%	1%	12%	32%	52%
Orange County	1990	2%	1%	10%	23%	36%
	1996	2%	1%	13%	27%	43%
	1999	2%	1%	13%	29%	45%
U.C. Irvine	1990	3%	1%	37%	10%	51%
	1996	2%	1%	47%	12%	62%
	1999	2%	0.5%	50%	10%	62%

These data were taken from US census estimates for California and Orange County and from data provided by the Office of Analytical Studies & Information Management at UCI.

The OAC (Office of Academic Computing)

Most universities provide services to assist students and faculty with computing and networking on campus. Academic computing services are relatively similar in purpose, policy, and services across university campuses.

Mission of OAC
In its catalogue, the University of California, Irvine (UCI) offers an explanation of the role the Office of Academic Computing plays on the university campus:

> The Office of Academic Computing (OAC) provides telephone, network, and computing services in support of research and education at UCI. OAC provides central computing services, computer laboratories, departmental and research-group support services, and campus-wide technical coordination. The campus network infrastructure maintained by OAC provides for Ethernet and higher speed connectivity on campus and to the world-wide Internet.1

The OAC's Mission Statement provides more specific goals:

> The mission of the Office of Academic Computing (OAC) is to assist the campus in the creation and maintenance of a computing and electronic communication environment that meets the needs of UCI programs in research and instruction. OAC's strategy is one of leveraging campus-wide computing and communication by providing:
>
> - Ubiquitous electronic communications infrastructure,
> - Basic computing and communications services to students and faculty,
> - Unique computer and network expertise and services best provided by a campus-wide organization,
> - Assistance to departmental computing personnel,
> - Technical leadership and campus-wide coordination for computing and electronic communication, and
> - Enhanced services to a few academic programs needing leading edge technical support.2

Campus Network
UCI utilizes UNIX-based systems in which students are assigned an account (an "ID") and password at a central location for accessing email and the Internet on campus. Specific email programs vary depending on what the student signs up for–such as Eudora, PINE, Netscape, or Outlook–but underneath any program is a series of UNIX computers, using passwords and logins that are maintained in a centralized file system.

Students can access the network from many on-campus public computing labs. These machine are usually personal computers that do not require login for individual use. Login is required, however, to take advantage of network services such as Internet access

and electronic mail. As an additional security measure, and to protect against theft and vandalism, many of the public labs have constant video surveillance.

The network is maintained by full time personnel of the OAC with the significant assistance of paid student help.

Computer and Network Policy
In addition to providing computers, software, and support to academic users within a college community, a subsidiary goal of campus academic computing services is to enforce computer usage policy. The Office of Academic Computing (OAC) at the University of California, Irvine (UCI) had implemented a Computer and Network Policy that all users were required to read before being given an account. Each user signed a document indicating they had read this policy. The policy encourages using university email services to share information, to improve communication, and to exchange ideas. The OAC provides a brief description of the aim of the policy that is helpful:

> The purpose of [the] policy is to assure that:
>
> - The University community is informed about the applicability of policies and laws to electronic mail,
> - Electronic mail services are used in compliance with those policies and laws,
> - Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail, and
> - Disruptions to University electronic mail and other services and activities are minimized.

Access to email is a privilege, not a right. Compliance to the policy is expected for all users, and failure to meet this responsibility can result in dismissal or revocation of this privilege.

Response to policy violations
The Office of Academic Computing (OAC) at the University of California, Irvine (UCI) has a Computer and Network Policy that all users are required to read before being given an account. Each user signs a document indicating they have read this policy. In the words of the policy, the purpose of the policy is to assure that:

- The University community is informed about the applicability of policies and laws to electronic mail,
- Electronic mail services are used in compliance with those policies and laws,
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail, and
- Disruptions to University electronic mail and other services and activities are minimized.

Access to email is considered to be a privilege, not a right. Compliance with the policy is expected for all users, and failure to comply can result in dismissal or revocation of this privilege.

The Computer and Network Policy defined at UCI specifically states an example of misuse to be "using computers or electronic mail to act abusively toward others or to provoke a violent reaction, such as stalking, acts of bigotry, threats of violence, or other hostile or intimidating 'fighting words.' Such words include those terms widely recognized to victimize or stigmatize individuals on the basis of race, ethnicity, religion, sex, sexual orientation, disability, and other protected characteristics."5 Masking or falsifying one's identity in an email is also used as an example, and is prohibited. The OAC lists among possible consequences the "temporary or permanent loss of computing and/or network privileges and/or Federal or State legal prosecution."

Although the OAC did not have a specific procedure to follow for each case of computer misuse that might arise, it did have an informal agreement worked out with the Dean of Students. In general, the Dean of Students' stance was that, once students had been admitted to the college, they have access like any other student to the various privileges on campus. If rules regarding those privileges are violated, privileges can be revoked. The OAC deals directly with any such cases, without contacting the Dean until it is an issue that is out of the scope of the computer use policy. In most cases, once a problem is identified, the OAC contacts the person, gets their attention by locking their access to their email account, and holds an internal hearing for the student with a few faculty and staff.

OAC Action

Dana Rood was the Associate Director of the Office of Academic Computing (OAC). It was the week before the start of theFall semester, and they were in the first blush of the hectic beginning of the term. Late Friday morning on September 20th he began hearing complaints from students about harassing email they had received. The first person he heard from was Elizabeth Doan, a female, Asian student who had been working in the lab down the hall from him and had received a message with the subject line: "Fuck You Asian Shit." She was accompanied by Jason Lin, who had also received the email. Jason had used the headers of the email to track the first message down to a particular computer, but when he went to see who was at that computer, it was unoccupied.

When the second message was sent, Jason again tracked it down, and the OAC looked for who was using the computer from which the second email had come. He and Elizabeth were now asking Dana what the next step should be.

The email headers indicated that the machine from which the first email was sent was labmac3, located in EG1122. The machine that sent the second message was pmac13, located in EG1140. He checked the login files to see who was logged into those machines:

rmachado pts/73 labmac3.acs.uci.edu Fri Sep 20 10:26 — 10:56
rmachado pts/29 pmac13.acs.uci.edu Fri Sep 20 11:10 — 11:47

The file indicated that Richard Machado was logged into each machine at the time the emails were sent.

At this point, Dana decided he had enough evidence to take some action. He contacted Allen Schiano, the core services manager in charge of labs, and the two of them walked down to EG 1140. They asked Mr. Machado for some identification, and he produced a student ID with his name on it. They then told him they suspected he was violating the computer use policy. He denied that this was the case. They said they would need to ask him to leave the lab and then asked him for a telephone number. Mr. Machado gave them a number (it later turned out to be false) and then left the lab at their direction.

Dana then locked Mr. Machado's account so that he could not access it. Because they had been worried about theft from the computer labs, the OAC had recently installed surveillance cameras in all the labs. Getting the video from the cameras would take a little while. Since they had dealt with the immediate problem and there were other things on his agenda, Dana decided to wait until later to resolve the rest of the case.

On Saturday, Dana read some samples of the offending email that had been forwarded to him. It was then that he began to realize that there might be more to this case than a simple violation of the email policy. The email had been sent to 59 people with Asian names. One of the lines in the email referred to the sender's intention to "kill every one of you personally." This certainly looked serious enough to bring in the Dean of Students'

Office, and perhaps the University or even the Municipal Police. He still didn't have the surveillance videotapes that would place Mr. Machado at the correct computer when the email was sent, and he wouldn't get that video until later that week. But the matter of death threats seemed urgent enough to require immediate action.

Student Response

Jason Lin worked for the Office of Academic Computing (OAC) on his student work-study award. He had worked his way up from the help desk to a student system administrator position over the several years of his employment. He was reading his email one Friday morning when he saw a message appear in the in-box with the subject header: Fuck You Asian Shit.

Irritated at this intrusion, he opened the mail and read the message from "Mother Fucker (Hates Asians)" <mfucker@uci.edu>. Its contents disturbed him, and so he looked at the headers to determine who had sent the mail and where they sent it from.

The "From" header had obviously been forged. This was easy to do in a variety of email programs and doing so was no mark of sophistication in an email sender. But other headers had not been altered. These were the ones that track the machines through which a message goes. He was able to see that the mail had been initially:

Received: from 128.200.69.203 (labmac3.acs.uci.edu [128.200.69.203]) by taurus.oac.uci.edu (8.7.6/8.7.1) with SMTP id KAA17113; Fri, 20 Sep 1996 10:54:31 -0700 (PDT)

which meant that the machine labmac3.acs.uci.edu was where the message originated from. This was just down the hall. So, he went to check if that machine was being used. There was no one there.

About twenty minutes later, he received the same message again. As he was reading it, Elizabeth Doan walked up to him and asked if he knew about the hate mail that was going around. She had received it too. This time, one of the email headers read:

Received: from 128.200.69.200 (pmac13.acs.uci.edu [128.200.69.200]) by taurus.oac.edu (8.7.6/8.7.1) with SMTP id LAA19557; Fri 20 Sep 1996 11:14:06 -0700 (PDT)

So Susan and he walked down to the lab containing the machine pmac13 (a different lab) and looked through the glass door of the lab to see a Hispanic male in a white t-shirt, light pants, sneakers, and a baseball cap sitting at that machine. The person was reading mail on a web browser.

James did not have an identity for the person sending either piece of email, since the From: headers had been forged. He and Susan then told his supervisor Dana Rood, the Associate Director of the OAC, that they had found someone who was sending inappropriate email in one of the labs in the building. John called in a colleague and together they asked Machado to leave the computer lab. They then locked his account.

Now the question was: where to go from here? Was the incident over or should more be done?

Legal Issues Regarding Harassing Email

University Policy
When Richard Machado sent his email to 49 Asian students at the University of California, Irvine (September, 1996) there were few legal restrictions on what individuals could do with electronic mail.

The Office of Academic Computing (OAC) at the University of California, Irvine (UCI) had implemented a Computer and Network Policy that all users were required to read before being given an account. Access to email is considered to be a privilege, not a right. Compliance with the policy is expected for all users, and failure to comply can result in dismissal or revocation of this privilege. The OAC lists among possible consequences the "temporary or permanent loss of computing and/or network privileges and/or Federal or State legal prosecution." Each user signs a document indicating they have read this policy.

The policy states that its purpose is to assure that:

- The University community is informed about the applicability of policies and laws to electronic mail,
- Electronic mail services are used in compliance with those policies and laws,
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail, and
- Disruptions to University electronic mail and other services and activities are minimized.

According to the policy, "using computers or electronic mail to act abusively toward others or to provoke a violent reaction, such as stalking, acts of bigotry, threats of violence, or other hostile or intimidating 'fighting words.' Such words include those terms widely recognized to victimize or stigmatize individuals on the basis of race, ethnicity, religion, sex, sexual orientation, disability, and other protected characteristics." Masking or falsifying one's identity in an email is also listed as a violation of the policy, and is prohibited.

The OAC did not have a specific procedure to follow for each case of computer misuse that might arise. It did have an informal agreement worked out with the Dean of Students. The Dean of Students' stance was that, once students had been admitted to the college, they have access like any other student to the various services on campus. If rules regarding use of those services are violated, they can be revoked. The OAC deals directly with any such cases, without contacting the Dean until it is an issue that is beyond the scope of the computer use policy. In most cases, once a problem is identified, the OAC contacts the person, gets their attention by locking their access to their email account, and holds an internal hearing for the student with a few faculty and staff.

Federal law

At the time of this incident (1996), there were no California laws regarding email use. Under federal law any threats of force that had the intention of interfering with specifically protected activities (e.g. voting, access to public education), was illegal. This law was called the Federally Protected Activities Act of 1968. Enacted in response to violent attacks on civil rights workers in the South, the act does the following:

> Prohibits intentional interference, by force or threat of force, with certain specified constitutional rights, including voting and election activities, participation in programs administered or financed by the United States, Federal employment, and jury service.
>
> Prohibits intentional interference with enrollment in a public school or college, interstate travel by common carrier, use of restaurants, lodging, gas stations, public entertainment facilities, and other establishments serving the public, State jury service and interference with employment (whether public or private), where the interference is motivated by discrimination on the basis of race, color, religion, or national origin. It also protects individuals who are helping others enjoy the free exercise of these rights.

The law does not mention the means by which this interference takes place, and so could be used to cover interference by means of electronic mail.

To qualify as illegal hate speech, a piece of speech must pass what is called the Brandenburg test. This is based on a case of Ku Klux Klan (KKK) speech in Ohio (Brandenberg vs. Ohio, 1969) in which Brandenburg invited a reporter to a KKK rally and the resulting video (with Brandenburg speaking) was shown on local and national news. The test was offered by the Supreme Court in overturning the Ohio law that made Brandenburg's action in giving the speech illegal. The test states that we cannot declare speech illegal, "except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."

Supporting Documents

Historical Documents

Headers and text of email Machado sent

On Friday, September 20th, 1996, Machado sent two, almost identical messages to 59 Asian students at UCI (University of California at Irvine), via email. The messages, with their headers, are included below. Recipients in the "To:" field have been omitted in order to protect the privacy of individual recipients. In addition, individual account names specified in the header information have been omitted.

Slight differences in the header information occur because the two messages were sent at different times, from different machines and because the headers are from two different recipients. The headers and mail were copied from poorly photocopied court records and may contain some omissions. All typographical errors in the text of the messages are in the original.

First message, sent Fri, 20 Sep 1996 10:54:31

```
Received: by mta4.nts.uci.edu id AA29475 (5.67b/IDA-1.4.4 for
{ommitted}); Fri, 20 Sep 1996 10:55:18 -0700
Received: from taurus.oac.uci.edu by mta.nts.uci.edu with STMP id
AA29429 (5.67b/IDA-1.4.4 for {ommitted}@uci.edu); Fri, 20 Sep 1996
10:55:12 -0700
Received: from 128.200.69.203 (labmac3.acs.uci.edu [128.200.69.203]) by
taurus.oac.uci.edu (8.7.6/8.7.1) with SMTP id KAA17113; Fri, 20 Sep
1996 10:54:31 -0700 (PDT)
Message-Id: <3242DB5F.4295@uci.edu>
Date: Fri, 20 Sep 1996 10:58:55 -0700
From: "Mother Fucker (Hates Asians)" <mfucker@uci.edu>
X-Mailer: Mozilla 2.0 (Macintosh; I; 68K)
Mime-Version: 1.0
To: {recipient list omitted to protect privacy of individuals}
Subject: FUck You Asian Shit
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Hey Stupid Fucker

As you can see in the name, I hate Asians, including you. If
it weren't for asias at UCI, it would be a much more popular campus.
You are responsible for ALL the crimes that occur on campus. YOU are
responsible for the campus being all dirt. YOU ARE RESPONSIBLE. That's
why I want you and your stupid ass comrades to get the fuck out of
UCI. IF you don't I will hunt you down and kill your stupid
asses. Do you hear me? I personally will make it my life carreer to
find and kill everyone one of you personally. OK?????? That's how
determined I am.

Get the fuck out,
MOther FUcker (Asian Hater)
```

Second Message, sent Fri 20 Sep 1996 11:14:06

Received: from ics.uci.edu by paris.ics.uci.edu id aa28498; 20 Sep 96 11:14 PDT
Received: from mta4.nts,uci.edu id AA06547 (5.67b/IDA-1.4.4 for {ommitted}@ics.uci.edu); Fri, 20 Sep 1996 11:14:59 -0700
Received: by mta4.nts.uci.edu id AA06473 (5.67b/IDA-1.4.4 for {ommitted}); Fri 20 Sep 1996 11:14:59 -0700
Received: from taurus.oac.uci.edu by mta4.nts.uci.edu with SMTP id AA06423 (5.67b/IDA-1.4.4 for {ommitted}@uci.edu); Fri, 20 Sep 1996 11:14:42 -0700
Received: from 128.200.69.200 (pmac13.acs.uci.edu [128.200.69.200]) by taurus.oac.edu (8.7.6/8.7.1) with SMTP id LAA19557; Fri 20 Sep 1996 11:14:06 -0700 (PDT)
Message-Id: <3242DB5F.4295@uci.edu>
Date: Fri, 20 Sep 1996 10:58:55 -0700
From: "Mother Fucker (Hates Asians)" <mfucker@uci.edu>
To: {recipient list omitted to protect privacy of individuals}
X-Mailer: Mozilla 2.0 (Macintosh; I; 68K)
Mime-Version: 1.0
Subject: Fuck You Asian SHit

Hey Stupid Fucker

As you can see in the name, I hate Asians, including you. If it weren't for asias at UCI, it would be a much more popular campus. You are responsible for ALL the crimes that occur on campus. YOU are responsible for the campus being all dirt. YOU ARE RESPONSIBLE. That's why I want you and your stupid ass comrades to get the fuck out of UCI. IF you don't I will hunt you down and kill your stupid asses. Do you hear me? I personally will make it my life carreer to find and kill everyone one of you personally. OK?????? That's how determined I am.

Get the fuck out,
MOther FUcker (Asian Hater)

Image of Machado from Surveillance camera

Authorities say they caught Machado sending the messages on this surveillance videotape (CNN)

Other resources

Background on email

This background document has two sections. In the first section, we provide some ideas about the psychological and cultural issues that influence our use of email. In the final section, we provide some basic advice you might want to keep in mind as you compose your email.

Its not all bad news

Since this case is about a misuse of email, we have been focusing on problems with email. But it is not all negative news. Email has become the primary mode of communication between people in many companies. It has increased the frequency with which older people interact with their families. It has allowed large scale cultural interchange. Much good has come from email and its large scale implementation.

Email and the culture of electronic discussion

Email is asynchronous. That means that I can send you email and you can read it at a later time. This is one of its advantages: we don't have to both be there at the same time. It is also one of its disadvantages. Since you aren't there I cannot see your immediate reaction.

Thus, email "distances" us from those with whom we interact: feedback is not immediate, and it does not contain many non-verbal cues that we use to make communication smoother. This distancing is not bad, but it can have effects that hurt communication. There are two effects that work together to make misunderstanding more likely and flaming easier to do (See Winter & Huff, 1996 for an overview of this approach).

First, we are distanced from those who receive our email because we do not see them directly, and because we do not see them directly react to our utterances. This lack of social cues in our communication means we do not get feedback about the effects of what we say.

Second, when we sit in front of a terminal, we can easily become wrapped up in ourselves and in our own emotions. Psychologists call this "self-focused attention." When this occurs, we can become carried away by our own interpretations and emotions.

Put these two things together: lack of social cues and self-focused attention, and you have a fine recipe for misunderstanding and "flame wars".

To this psychological level of analysis, we can add a cultural one. Discussion groups on the Internet form their own rules and sanctions about behavior (Finholt & Sproull, 1990). They may expect people to be either rowdy or calmly professional. They will have ways of punishing those who break the expectations. Thus these groups become small (or very large) social venues of their own. The difficulty is in learning how to switch from one venue to the next.

Some practical advice

We are beginning to see some convergence in the recommended rules for interaction over electronic media. "Netiquette," simply put, is network etiquette–a set of rules guiding proper behavior online, encouraging respect and consideration of others utilizing Internet services, especially email and newsgroup postings.

Numerous sources have been created to help provide information about netiquette. Several different approaches have been made, because the net presents a tremendous range of possible problems regarding proper behavior. In her book entitled *Netiquette*, Virginia Shea (1994) identifies ten core rules that should be considered when using electronic interaction:

1. Remember the human–It can be easy to forget that there is in fact a person behind the computer screen. When writing an email, for example, consider the question "would you say it to the person's face?" to determine if you are engaging in proper behavior. Also, remember that any email you send or receive may be saved or forwarded, with or without your knowledge.
2. Adhere to the same standards of behavior online that you follow in real life–Just because you are working behind a screen does not mean that ethics and the law no longer apply.
3. Know where you are in Cyberspace–When you reach a site, get a feel for where you are; netiquette varies from area to area.
4. Respect other people's time and bandwidth–Bandwidth refers to both the machine capacity for transmitting information and to the individual's time capacity to read and understand it. It is important not to send unnecessary emails and information that will exceed this limit. Also, be mindful of your mailing lists–send emails only to those whom you are certain would want to read your message, as extras only fill up another person's mailbox.
5. Make yourself look good online–The anonymity of online communication can be a positive quality, in that users are not judged by appearance, status, etc. But, this also means that more weight is then given to the way you present yourself in writing. Thus, take care to know what you are talking about, and to make sense. Also, don't post flame-bait. "Flaming" refers to the act of expressing a strongly held opinion online, often done in chat rooms and/or discussion groups.
6. Share expert knowledge–The Internet essentially saw its beginnings in the exchange of useful information among scientists and other professionals worldwide. This is still an extremely unique aspect of the Internet; if you are capable of sharing your knowledge with others, don't be afraid to do so.
7. Help keep flame wars under control–Since flaming isn't forbidden online, users must take responsibility to keep it under control. The perpetuation of flame wars–a series of angry responses, usually among only 2 or 3 members of a discussion group–is in fact frowned upon. Aside from being offensive and especially boring for those in a group that aren't involved, flaming monopolizes bandwidth as well.

8. Respect other people's privacy–Email is just as personal as the contents of a desk drawer or file folder. When you forward someone else's email, make sure to get their permission. Going through another person's email is extremely unethical.
9. Don't abuse your own power–Some people simply know more than others who are in Cyberspace. This kind of power does not give you the right to take advantage of others.
10. Be forgiving of other people's mistakes–Being that the Internet is still a relatively new medium, mistakes will undoubtedly occur. Not everyone in Cyberspace has had the opportunity to learn the rules and regulations. Thus, it is necessary to be respectful when others make errors. If you do point out a mistake, do so politely, and in private rather than public if possible.

Transcription of Interview with Dr. Schiano

S: Hello?
C: Hi Dr. Schiano, this is Christina Harmon from St. Olaf college
S: Ahh, you're on speaker phone (laughter) hello there
C: Is that still okay with you, if you're on speaker phone and being recorded…?
S: No problem whatsoever. Hold on one second while I close the door….yes, hello, I can hear you…
C: Alright you can hear me okay?
S: Yeah.
C: Great. I just wanted to talk with you a little bit today about the project that I'm doing and a few things that I wanted to fill in that I couldn't without some input about your OAC, or I guess it's called NACS now, is that right?
S: Yeah we just changed it…ah…4 days ago.
C: Okay, did I make sense when I explained what our project was about, or would you like to hear more…?
S: Little bit–you're doing a research project on, what is it, computer ethics?
C: Yeah, it's going to be–well it already is a website, but there is going to be a lot more…
S: Okay, well I haven't seen the website, but I'll take a look at it.
C: Oh, that's okay, it doesn't matter–the website it going to be used in computer science classes by professors to teach their students about ethical and social issues in computing. The way that they're going to learn is through all these different cases that we're presenting, and the one that I'm working on mostly is Richard Machado.
S: Okay.
C: So, Sara Kiesler over at Carnegie Melon was nice enough to give us 4 huge binders of all the different information–exact testimony, and things about the case, and so there's a lot that I know already–but…
S: Have you talked to anyone here at UCI?
C: I haven't.
S: Okay, because I talked to my boss Dana Roode who was more closely–actually, we both were–but he was the one who did official things about it. The other person's name is John Ward. He's the system administrator who testified as to the steps we took to identify him.
C: Okay…see that part's missing from our…
S: Yeah well, and since I don't know what you have, I was involved in the background…and…I remember parts of it, but it's been a long time…so, I may have forgotten all sorts of parts (laughter)
C: That's okay…There are certain parts of the case that I'm interested in, but there are actually things that I'm especially interested in just about your computer center there…so, I did e-mail Dana Roode and Liz Doan who was a student at the time, and you, and I heard back from you…so…
S: Okay, who's the other person you e-mailed?
C: Umm, Liz Doan–
S: Liz Doan, right–she was one of the recipients of the e-mail…works for us…

C: Yeah…Well, one of the things I was interested in was just understanding your network on campus a little better, your e-mail system, because I was reading through the description on the web, and it sounds like you guys have a lot of options for students.
S: Okay, you wanna know at the time that this occurred, right?
C: Yes, and now–I want to know both, because I want to know what's changed.
S: Okay. Umm…about 1990 or maybe even earlier, I don't know, I've been here since 1990–somewhere along in there, we've always had e-mail accounts for students available…at the time when we first started this, the students would sign themselves up, they would fill out a menu on a terminal that would basically ask them questions and they would be assigned an initial password and they'd have an account on the computer.
C: Okay. So was it like UNIX, or Eudora…
S: Ah, in the background it's always been a UNIX computer–in the front what they were seeing, initially, was a program named PINE.
C: PINE, okay we have that here too.
S: Okay, so they're seeing a little program that has little menus. We basically wanted to go with something that was not too complicated for them–not too many options and whatnot.
C: Right, so that's what Machado was using?
S: No, haven't got there yet…ahh, that's what we started out with. Over time the demand kept going up and there started being instructional uses for such, we moved to a model where all students were assigned information based on what the registrar would give us, that's what we're currently doing at this point. And same thing with faculty and staff through different data bases.
C: Yeah, that's what I got out of it…
S: Right, so we would assign an ID to all of them, and underneath is a thing called "curburos" [phon], which a lot of places use, which basically assigns them a password in a central location and based on that we would then create the UNIX computers essentially that would manipulate their e-mail. And then what people would use to access that e-mail over the years has migrated as more and more people use PCs. So using ah, Eudora, Netscape, Outlook, lots of different ways to get e-mail. But then down below is a series of UNIX computers that are using local passwords, ah excuse me, passwords and logins that are maintained elsewhere. Okay, so that's part of the e-mail. The other part is where do they go to actually see this e-mail, and there are computer labs all over the campus, and there are computers in people's offices…generally the students go to the labs or they log on from home. So in his case, his use of e-mail was in our labs, and maybe elsewhere, I don't know…I don't remember…that he would be using PCs that we owned and using Netscape.
C: That's what I thought…okay…Because they had mentioned in the documents that he had used the "finger" command to determine who he would send this e-mail to…and I've played around a little bit with that…
S: Yeah…what he had done, what we'd determined–but like I said I wasn't involved in the court proceedings at any time, except that my employee John Ward was there, testifying and providing information to the FBI, and DA and whatever–what we determined was that he had been a user of these systems for a long time like all

students, and he possibly could have used IRC, Internet Relay Chat, which is a chat-room program, that's available to them, although we don't really like it–people to use it–to identify some people. He had used finger to figure out who was logged on. So he knew a little bit about the access he could get through a UNIX shell–which is what the students have access to, and of which they can use PINE, or IRC or type finger, things of that sort–so he was getting info about who was logged on about the people that he was talking to in e-mail, or in the chat room. So he had done that and he was using the labs at the same time to be sitting in front of and to be running these programs. He apparently had determined how to use Netscape–in fact some of the early messages that he sent were tests–to show that he could forge an identity.

C: Yeah, that was my next question–he changed his address field, right?

S: Right, he changed his address field in Netscape, which you can do, and use Netscape to talk via POP, to our mail servers, changed his name and called himself something else. He also included himself on the "To:" list, and there were lots of funny things…He had included a person on there at our medical center that he had found whose name was I think "Korea" or something, who turned out not to be Korean at all. So he was basically pointing out Asians of various kinds, and he had found them, and he had tried a couple tests, and then he sent out the message, and then he sent out a follow up one to the same group saying "I just got this, isn't this bad??"

C: (laughter) Yeah, "he thinks I'm Asian," or something like that…

S: Right, so he tried to distance himself, so that's what he initially did. While we were, what had happened at that point was that he'd sent this message out to 50 or 60 people, some of them were our employees. Liz Doan is one, she's the one who actually testified, there were a couple others as well who didn't really want to get too involved, so there was a lot of apprehension of actually getting involved in it. But some of our employees got the e-mails, and one of them worked in fact for one of the system administrators we have, and he was quite good about this, and he started figuring out where it came from…The computers, the way e-mail works, the computer that you sit in front of, and the Netscape session that this occurred from pointed to a particular PC in the lab. So he didn't know it was R. Machado, but he knew it came from that machine. Then he was very resourceful and figured out who at the same time had logged into the computer running finger and whatnot, because he [Machado] didn't have to do that, he could've just gone to Netscape, unaffiliated himself, unlogged in to any other accounts on the computers, and just run Netscape and we wouldn't have known much more about it. But the fact that he was also logged on to the UNIX box at the same time, we put two and two together figured out it was that computer, and that ID–we call it the UCI net ID–of that person, sitting in that spot, with that name! (laugher) So at the point he [the employee] came upstairs and said "there's someone down in here that's sending hate-mail, sending mail of some sort" — so I'll take a break here and describe something else…we have a policy like most universities who've run into any problems like this or anything much more minor than this, ah, a computer use policy.

C: Yeah, I was going to ask about that too.

S: And we have developed one from other universities' that have developed, and what we've been hearing about lawsuits, what laws should be, etc, so we developed a policy

about usage. It specifically says a variety of things–it may have been in fact in the documents you have, and it's online, it hasn't changed…

C: Yeah, I think I do have that…

S: And it basically says "Thou shalt not do certain things" or you'll run into all sorts of problems. And we worked that out with our campus Dean of Students, as to–that's our way of doing the Dean of Students' work for these things–basically our equipment that we have…it's up to us to decide what inappropriate use is, of the systems themselves, like someone running a program we don't want them to, that we told them not to, but we also have the responsibility to work with the Dean of Students and the campus judicial sects when there are things that occur that go beyond that, like ah, public indecency--We've just been dealing with a case of public indecency in the laboratory, so that goes beyond campus to criminal law, so we have to, we help them with that job and they've assigned us the ability to do that job of, when someone does something wrong it's equivalent to someone cheating on an exam or…ah…handing in somebody else's homework, we basically could say "these are the penalties." So having said that, when the student came up and in fact talked to me first saying "someone's sending me hate-mail, and I know who it is" we identified the system administrator and I'd gone down with him to point out where the person was. And at first I thought it was essentially just someone sending an, ah, annoying e-mail of some kind–"I don't like you," you know or ah some poor language which is something part of our policy that is not allowed. Profane language, how's that? I thought it was just profane language. And so, ah, at that point, I went with him and saw where the person was, and at that point, also other people had started coming upstairs and saying "I'm receiving this as well," and my boss at that point, Dana Roode and I went downstairs and Dana talked to Richard Machado and asked for his ID, and there's a video tape of this because we have surveillance tapes…ah, asked him who he was, etc, and said, you know, "you've been using this equipment wrongly, breaking our computer use policy," — at that point neither one of us actually had read the e-mail. What we had heard was, you know, "using derogatory terms, sending bad-mail" or whatever. We didn't actually sit down and read it. That was, in hindsight, one of our mistakes. We should have looked at it more carefully, but we basically told him to leave the building and he left. After that, the e-mail started getting around and over the weekend my boss read the e-mail in detail, Dana did, and on Monday morning we called the campus police.

C: Okay–that's something we were confused about, because we knew that he been asked to leave on Friday and then nothing else…

S: Right, no one had really read the e-mail. It went by wild-fire over the weekend–people had received it and said "this is more serious"–in fact someone had talked to me, one of my staff, who's background is Japanese-Hawaiian was very offended that this had occurred, and then we called the campus police. They then called the DA and it went from there.

C: Okay, so it was kind of just more that nobody understood how serious it was when it happened?

S: Yes, yes. The people who received it, ah, some of them didn't pay much attention to it, some of them got very concerned. The person who had come to us first–it was one of our employees, and it wasn't Liz–essentially just thought this was just within in reason or whatever. When the people who normally–ah, John Ward who was applying the

policy and monitoring the usage at that time–by the time on Monday we all got together and realized it was much more serious. So the delay was over the weekend and the fact that we didn't read the message. We get a lot of people saying "Yeah someone sent me mail with curse words in it," and that's what it was assumed to have been. But when we actually read the threats–you know, "I'm gonna kill you," and the fact that he had sent it to 40 specific people, the details are important too, it wasn't just sent to a newsgroups anonymously and whatever…

C: Yeah, he'd taken great care…

S: In hindsight, I never met him, but this was very foolish and stupid. He didn't know what he was getting himself into at all. Then if you read the rest of the things that were going on in the community, I have to describe UCI a little bit–UCI is about 30-40% Asian-American or actually Asian nationals coming here for instruction. So there's a large Asian contingent at the University. Orange County itself has a large Vietnamese ethnicity–several hundred thousand people–and a comparable size of other Asian cultures in the county. So it hit in an area where there was a lot of sensitivity to anything like this. So that caused campus and communities groups to get up in arms–the fact that it went to 60 people, and the local FBI got a hold of it very quickly, and it seems to us in hindsight that they were looking for, they had seen lots of hate-mail incidents in the LA area, and they were very attune to such things. This one was just unusual being an e-mail. So it basically mushroomed in a hurry! (laughter)

C: Yeah…Would you mind if I asked you a couple questions just about your procedure in general?

S: Sure.

C: So it sounds like there's not really...ah…you don't go to the Dean then?

S: Well, let's say–let's get a better example. Ah, we find out–we get a complaint that someone has received an e-mail from an account or an account seems to be in a weird state. So, we will then ask the person responsible to come here, or in e-mail, "did you send this e-mail?" — usually we ask them for an interview, and how we get them in an interview, we lock their account to get their attention, because they basically work with e-mail only. University students don't usually give us access to their home phone numbers, we don't use that information, so we use their e-mail account, locking it to get their attention, we have essentially what amounts to a hearing, to figure out what has occurred, and it's to find out if something serious has occurred, like an account has been broken into…

C: Now is this a hearing within the computing…

S: Within, yes, with the system administrator and maybe a few staff at most here, acting as lieutenants to the Dean of Students. Our job is essentially to find out what did they do to the equipment that we're responsible for? We often get people who will, say, share a password, and that's a definite no-no. But they do it, you know…so we try to determine if it was something where they violated policy, or is it something more serious, like did someone break in, or did they break in? Based on that, we make a judgement, "Well, you shared your password, you should have known better, you didn't read the rules" — We force them to read the rules when they log on–they can't get an account unless they physically read it and answer a few questions. If it's a sort of moderate level case like I said, with the password being shared, we say "well, no account access for two weeks" or something. If it's more serious than that, then we

advise the Dean of Students, and they're usually, they're pretty draconian of making people doing community service–they're used to people stealing things. So they're going one step before calling the police. Or they'll call the police, and sometimes we'll do it directly ourselves. But most of the time, it's essentially an internal hearing, making sure they've read the policy, they understand, at the same time try to figure out exactly what the incidents were.

C: I think that sounds like a really beneficial procedure…

S: Well, there are still lots of pieces that people have difficulty with–universities have this problem–getting all the info out to all the students, that this is the responsibility, it's not for free that they have a right to it, that they have responsibilities not to do a lot of things; people believe that anything's okay on the web or an e-mail, and it's not.

C: Right, that's part of what we're trying to target.

S: Yes. Not everything is okay, and a lot of things cross the boundary to criminal activities, and the FBI are very interested in such these days, and I think in the case of Machado, he had no clue. He added to his misery–they probably would have let him get off with some probation or whatnot, but he skipped bail, went to Mexico, they found him again as a fugitive, that added to his woes, but because now he was in jail, when they finally found him guilty, it was essentially "well, you serve time"–and we haven't heard from him since! I don't know what happened to him…Umm, it's the worst case we've had in terms of dealing with, following this through, but we've had hacking incidents where we've traced it and had the police come in, students have been expelled–not many–but, people have been suspended, but…it's equivalent on a college campus…the same thing as people cheating on tests, the worst cases you have…it's very similar.

C: So policies and penalties are pretty case-specific then, right?

S: Well, we have a list, it's not public, but it's something we share with the Dean of Students and the people coming along, essentially a penal code as to what we do--

C: Oh, okay.

S: --and some of the things are just administrative–if we don't want you to write a file in a particular area because it causes trouble, we tell you don't do it, and if you do it once, it's a warning…If you do it many times you're not paying attention and we lock your account, take away privileges. So getting access is a privilege, not a right. The basic description that the Dean of Students will say–these are UCI rules–that, ah, once their students are admitted to the college, then they have rights like any other students to the various things on campus, unless they get themselves in a situation where they're basically denied those privileges. If they break a rule that we set, it's our responsibility to say "No, you don't need this" — where it comes up very difficultly in an academic setting is more and more instructors are using the web and e-mail and whatnot to communicate with their students, and in those cases what it ends up being is students have been told they no longer have an account, and you need to tell your instructor ahead of time, and they'll need to do something else.

C: So then, what is the liability for the NACS?

S: Well, you mean if they're being sued by the people or something?

C: Yeah.

S: Well, again we're representing the University and the policies we set, we have to be specific about writing the policies we use, and we have to follow a due process where

we allow the student to say what's going on…We have to communicate that to the Dean, so the Dean knows that's what we decided upon, and that about covers it. The various things that we give out are not any kind of rights, as I said, the services we provide–in terms of something like the Machado case, we generally will just turn it all over to the campus police, and the Dean, who basically take it from there, so we're representatives mostly to the Dean but not to the police dept., but it just goes off. So our liability is not necessarily to us identifying them, but the steps we have to take are that we're not discriminating against them, that we're applying the same rules to everyone, and that we're stating what those rules are, and that's what they sign-off at the beginning, saying "yes I have read this policy." Ah there's one other thing–I talk too much, I need to let you ask some more questions–the other one that we're trying to do is, we've sort of stream-lined this a bit, to make the people who actually investigate a lit more formal, with a penal code and a set of rules. In the past in was little bit more informal–the system administrator would write these things down, but they'd be like the only agent. They'd come to their manager if there was someone who wanted to talk to the management or something like that. The other thing that we're doing that's maybe kind of interesting and unique is, we realize a lot of these issues are minor. There are things like "even though I gave my friend my login," we're worried more about it's consequences more than the actual act. So we've set up what I've called a "Computer Traffic School," which is essentially–all the things that are minor we make the students go back and go through and read questions related to the computer use policy and answer them appropriately, or if they don't, keep answering them until they get it right–so it forces them to sit down for maybe a half hour in our areas, going through this again.

C: I think that's a really good, good idea.

S: Well, I think you've got to do that because most of them are in fact minor so you're worried more about big things happening, but you want to make sure you educate people and you can't just do things like "Oh, go read this, it's over there"–they don't. You've got to get them to sign something off–that's where you get the liability issue as well–you said you read it.

C: You kind of touched on something I was going to ask, you said it's kind of new, and I was just wondering how much or what in your policy has changed since the Machado case, like penalties and that sort of thing.

S: No, nothing since this is so far outside the range of it–there's nothing that says "Thou shalt not send hate mail," anymore than it says "Thou shalt not be indecent in the lab"–right now we're dealing with a situation where someone in the lab was indecent, probably even worse than that, but I'll leave that to your imagination–and he went off to court and he was tried in court today and found guilty of doing various things in our labs that other students were seeing. Now that's not something we're going to write in our policy, you can't violate the laws of the state of CA in the US penal codes, so we're not writing down the worst case scenarios, and in the Machado case, there was really nothing to write down. The only thing it taught us is that these things can be more serious than at first, and doing things like reading the message or assuming that the message is of one kind when it could have been something else. And then part of the whole legal case was, is this just a normal flame or is this in fact hate-mail, or a

criminal activity? And in fact the actual regulation is quite fascinating, that was used by the federal government on him was a law from 1968, or was it '63?

C: Oh, I didn't know that part.

S: Yeah, well the actual part that was used was that in the federal statues–and this comes back from the civil rights era–that no one will have the right to abridge the access of any citizen to public institutions of learning based on sex, race, creed, etc. And what they were saying essentially was that by scaring these students that there was somebody here willing to kill them was abridging their right to come to the University. So that this was a constitutional rights case. And that's in fact what they tried him on. And that goes back to the 1960's with the various black students being not allowed to go to Universities in Alabama, Louisiana, being barred by the governor. So it was in fact a very serious law, nothing minor, people were killed over this. So that's what they had said that he was trying to provide fear and it wasn't just a flame because he'd picked out particular people, he had looked to see if they were Asians, it wasn't just a message in a newsgroup that was known for people flaming each other left and right and saying, you know , "I don't like the Japanese," or "I don't like the Romanians" and being very bland. This was "You particular, I'm gonna come and kill you," and that crossed that border, and that's something that, you know, computer folks don't spend much time on.

C: Right, and that's another thing–I noticed that when they convicted him that it wasn't at all, like you said, about anything having to do with e-mail, but something broader, and they applied that law to an e-mail case. I've done a lot of looking into laws about e-mail, but like you're saying, there doesn't seem to be a lot of concrete stuff about harassment or threats like this, do you know–

S: Yeah, that is in fact why the federal government and the FBI and the US DA were heavily involved in this and I think it went all the way to Janet Reno at some point–it was because they wanted to set law. They still continue to want to, in the justice dept., wants to set definitions.

C: But they haven't, right?

S: Ah, well I wouldn't know…I'm not a legal expert, but nothing has come to us. We have a campus e-mail policy now, a UC-wide policy, but it generally deals with things like, who has access to your e-mail if you're an employee or a staff member. Those are more issues of access because they're worried about liability again. The actual issue of freedom of speech, as far as I can tell, hasn't really been defined much more. So what they were applying were existing rules to show that e-mail is no different. And essentially that's what the sort of policy we follow in general–just because it's an e-mail conversation of some sort, that's no different than if it was a personal conversation. You know, that's like if someone sends you regular mail and you open it up and it's addressed to you and it says "I hate you, I'm gonna kill you," the post office wants to know. (laughter) So they'll go and do things about it, and there's a long tradition of regular mail and regular communication, so they wanted to set policy here that's saying e-mail is no different. And as far as I can tell no one has made a counter-judgement, but I don't think it's gone like to the Supreme Court or anything but I don't see why it would be judged any differently actually. There's nothing really different about it–there's this belief that the Internet is wide-open, but you still don't go around and flander people or ah threaten them, that hasn't changed. It's just that there's easier

opportunity of telling a whole bunch of people through something like your website what you think. So the Machado case hasn't really affected us, except internally of being more careful.

C: Yeah, sure–umm, one of the last things I was wondering about was that, we, just to understand it ourselves a little bit better we were trying to figure out a little more about his background and we haven't found much and I was wondering if you knew of anything…

S: Umm, all we knew was what we knew from the registrar and the police–he'd been a student here a couple years already, the Orange County Register put a lot of effort into this and we spent a lot of time talking to their reporters and they'd spent a lot of time trying to figure out his background, why he'd do this, etc, so I'd aim you maybe in their…they have a website as well, I think it should be either ocr or ocregister but they have archives and whatnot. Their reporters there, I can't remember their names, but they were around quite a bit. But the ah…what we knew from the papers essentially was that he'd been a student here, his grades had been failing a bit, he was depressed about a brother of his who was killed in some event, and those were the things he said in court that affected why he'd want to do this. As I said, the University has a large Asian contingent of students, there's probably feelings of bigotry on both ends and obviously that came up and that's why they thought this was a racially motivated hate crime, he picked on this group. This University is a little unusual it got a reputation in the early 60's–it's only been here since 1965–St. Olaf's has been there a lot longer, I know that!–but ah, it's not been here a long time, it got a reputation for being, ah, it was a new school, so it was less traditional than Berkeley or UCLA and it also started out more of an engineering school and but it isn't really that way now, so people migrated through this area who were interested in computers and engineering and whatnot and, I don't know if you want to attach any racial bias to that…and because the community too has a large Asian contingency, it's not really that unusual for the county or California. So, I don't know why he came to this University, what his major was…Don't know what happened to him. It really was sad because he didn't know what he was getting himself into, this was not a situation where this was developed for years, he wanted to use this as a sounding board for his views, he had apologized profusely in various public events that were staged by the campus to basically try to diffuse the situation, but then the federal government wanted to use this as an example and so the DA just followed along saying "yes, this was a crime."

C: Well, and I think that's a good point to make, because we are trying to, especially for students, help them understand that exactly–that things like this happen and you don't realize what you're getting yourself into when you're doing with it…

S: Yeah the way we describe the authorization part, the password and login, to students is "This is like your PIN on a credit card"–would you give this out to anybody? Your best friend could get on your account in a few minutes, send mail to the president of the US, saying you personally were gonna come and kill him, and the security would be here in minutes! (laughter) So you don't want to identify yourself–to give them things like, it came from your account, with your name, your password, you don't want to give them that. Because people do things like that, and this is no different–it's not as open as they believe, there's just as much responsibility as anything else. So that's the most important thing I think I would tell anyone about this case or this in

general is that, you have responsibilities to ah the same way you would do a variety of things for the same reasons for other mediums. It surely allows you to communicate quicker with large numbers of people in a variety of ways, but then there's even more responsibility. It's like SPAM–you can easily send mail to hundreds of thousands of people and you may thing "oh that's no big deal," but then all the computers along the way have to process that, and that slows everybody down and they don't get something important and it's all because you played a joke and right now people are–commercial companies are suing people left and right that send huge amounts of SPAM and their winning cases. So there could be serious financial consequences for something as simple as that. A lot of responsibilities.

C: Yeah. Okay…

S: So good luck to ya!

C: Yeah, thanks! Is there anything I didn't ask that you'd like to touch on–I think that pretty much covers what I had…

S: Umm, no I'd say look at our computer use policy, there are other universities that have them…If you wanted to look some more into this particular case, I'd contact the Orange County Register Newspaper–either ocr or ocregister.com–or use some search engine.

C: Oh great.

S: They'd go into a lot more detail, and in fact maybe even a reporter could talk to you about it. Ah, Dana Roode my boss is out of town for about a week. What he would add to it maybe is his personal interaction because he had to testify and give information. He had dealt with the media–they descended on us like nuts from all over the country. And John Ward would be able to tell you more about the specifics–he's not back 'till Monday. You can find all our phone numbers and e-mail on our webpage, so…

C: Okay, well, thank you so much — you've been incredibly helpful.

S: Sure well good luck to you–when you write something up tell me about it, love to see what you said.

Analysis Documents

Socio-technical System

What is a socio-technical system?

A socio-technical system is a conceptual tool we use to help us understand the entire system within which any particular computing system is embedded. The ethical issues hardly ever arise about disembodied, abstract, systems. Instead, ethical issues arise when a computing system comes into contact with the real world: thus socio-technical system. If you need some more background about socio-technical systems, we provide an overview.

But for now, simply remember that a socio-technical system can include hardware, software, physical surroundings, people, roles, procedures, laws and regulations, and data and data structures. As you can see, a socio-technical system can be quite complex. In this document, we will help you discover some of the more important pieces of the socio-technical system surrounding the Machado case.

An overview of the pieces

Machado's message was sent on a computing system that used the Unix operating software and network protocols. The mismatch between the collaborative cultural environment in which Unix was developed and the large, institutional culture in which Machado used the system is a central player in the case. Thus, this software, its procedures, and the culture that spawned it are important parts of the socio-technical system.

The Office of Academic Computing (OAC) was the primary administrative structure that has responsibility for the network and computers that Machado used, and thus their personnel and procedures are part of the socio-technical system.

Machado used a style of writing called "flaming" that originated in discussion groups on the Internet. It was through such discussion groups that Machado learned this style. The social assumptions of these discussion groups thus become an important part of the socio-technical system.

The University of California, Irvine (UCI) is a relatively young university, dedicated to providing a place where students can encounter each other and the world of ideas. Thus, the rules and social expectations of the university system become an important part of the socio-technical system.

National law enforcement became involved in the case, after it became clear that Machado could be tried on the grounds of violating the civil rights of the Asian students he threatened. Finally, Machado’s personal circumstances interacted with all of these pieces.

The parts of this socio-technical system are intertwined: Unix software and networking protocols, the culture of online discussion groups, and university culture are all closely related and inherit rules and expectations from each other. Discussing one will likely lead to discussing several. You should not merely tolerate this complexity, but look for the patterns within it so you can welcome it.

The Unix computing culture (from which smtp and finger emerged)

Unix is an operating system first conceived of in 1969, and that has been continuously evolving since that time. An operating system is responsible for all the basic operations of the computer (at that time, a DEC PDP-7) including the file system, ways of interacting with files and peripherals (printers, screens, keyboards), user utilities (like copy) etc. Oddly enough, it was first designed to serve as the underpinnings for a game called "Space Travel," but it quickly became evident that its potential was far greater. It was called Unix in what Dennis Ritchie (one of the designers) has called a "treacherous pun" on the system it was designed to replace: Multics.

Thus, the Unix operating system was born in a computing research lab, to serve the esoteric needs of computing researchers. In the early to mid 1970s, it was widely adopted by academic computer scientists. Its wide adoption can be explained by several factors:

- It was a flexible and robust operating system
- It was inexpensive
- The original designers of the system were open in discussing its operation and adapting it to different environments,
- It served as a good teaching tool (it was mostly written in a high level language called "C," and you could use the system while studying the programming language and rewriting the system itself).

A culture of cooperative computing arose around the development and study of Unix and C. Academics (at Berkeley, Stanford, Purdue, Univ. of New South Wales), and researchers (at various Bell Labs sites) shared their problems and insights on the system and negotiated together what they thought the best implementation of the system would be. Disagreements produced alternative versions, but substantial cooperation was a hallmark of the community.

Networking became practical with the advent of uucp (Unix-to-Unix copy) and electronic mail became a way for these researchers to communicate with each other. As networks became more sophisticated, a series of protocols were established using a procedure called "Request for Comment." These RFCs were public documents that took advantage of the collaborative atmosphere and structured the discussion by focusing it on a document until there was general agreement on the standard. This procedure emphasized collaboration among colleagues.

Finger

Finger originated at the Stanford Artificial Intelligence Laboratory in the mid-1970s. Because collaborating among programmers was an important part of the culture, it

seemed like a good idea to be able to see who was on a system at any one time so you could ask them questions or get them to problem solve with you. Finger was designed to show you whether a particular person was logged on at that time, where they were (what terminal they were using) and other useful information about your programmer colleagues. If you typed the command without listing anyone, it showed you all the people who were logged on at that time. Again, this was useful to find out who else was up at that time and on the system.

This system command, designed for use among collaborating colleagues, was used by Machado to target individuals with Asian sounding names. He simply entered the finger command without any arguments and found all the people (and their login names) who were logged on at the time. Since a standard, friendly feature was to have login names reflect your real name, Machado could use the login name to look for people who were likely to be Asian. Here we see that a computing system designed under one set of assumptions (friendly interaction among programmers) can become a severe liability when it is used in ways that violate those assumptions (to target people for harassment).

Recognition of this issue is evident in the change in tone of RFCs from the early implementation of a network-based finger command (RFC 742 from 1977) to a much later implementation (RFC 1288 from 1991). The early RFC makes no mention of privacy issues or other difficulties, while the 1991 version has clear and direct warnings about the problems you can get involved in when you implement a finger server on a networked system.

SMTP

Simple Mail Transfer Protocol was originally established in 1982 with RFC 821. It defines it goal as "transfer[ing] mail reliably and efficiently." It is technically based on TCP (transmission control protocol) a part of the early ARPAnet's Department of Defense standards. Efficiency and reliability are the watchwords here (as they were for all the ARPAnet projects).

For instance, a time stamp line was to be inserted as a new header by every machine that handled the mail. If User1 sent email to User2, it might not go directly from one machine to the other (since there might not be a direct connection, or forwarding might be set up). But as it moved from machine-a to machine-b to machine-c each machine using SMTP would place a new time stamp header on the mail showing the date and time it had been received, and the identity of the two machines. This tracking helped in answering two questions: "How long did the message take to get from each machine to the next?" (efficiency) and "If it failed, where in the chain did the failure occur?" (reliability).

The issue that the Machado case brings up is the mismatch between the Unix culture that valued efficiency and collaboration and the UCI culture that required surveillance cameras, security measures, and tracking. The SMTP headers that were originally designed to serve as efficiency markers became security trails that allowed the OAC to track down the original sender of the hate mail. Thus a computing system that was

designed under one set of values was used by people with a different set of values for purposes not originally foreseen.

The Office of Academic Computing (OAC)

The OAC was a long way from the small, friendly groups of computing researchers that formed the early world of Unix. Like most academic installations, they used Unix as their primary operating system. But they also had hundreds of open personal computers in labs all over campus in an urban area. They had thousands of users on a modern university campus with a great deal of turnover in the student population.

In response to this logistical nightmare, the OAC had implemented policies about appropriate computer use (see the OAC background document in the case narrative). In addition, they had mounted surveillance cameras in their computing labs so that they could videotape the people in the labs. This combination of measures helped them to catch Machado when he sent his hate mail.

But they were still running an implementation of the finger program, and this allowed Machado to find his targets. There were procedures in place that worked on most cases, but in this case, led to a short delay in catching the author of the hate mail. The two administrators for OAC did take prompt action to remove Machado from the lab when the incident was reported. But they did not actually read the email in the incident until at least the next day. Upon reading the death threats in it (the students who reported it had not mentioned these) they decided that it was a matter for the police to handle.

The incident then rapidly escalated until the FBI was involved in prosecuting a federal civil rights case. Thus we have three worlds coming together, the Unix computing culture, the modern university, and the legal system.

The world of online discussion

Online discussion forums range from the dryly professional to the raucous and outrageous. Some discussion groups are specifically set up to facilitate what is called "flaming:" long, ranting, messages that personally attack those with whom the author disagrees. This form of argument by name-calling is usually frowned upon in most Internet discussion groups, but it occasionally rears it head, gets labeled "flaming" and those doing the flaming are asked to quit.

In some ways, the mail Machado sent out was the classic flame. Much of it was in all capital letters, a classic form of electronic shouting associated with flames. Many vulgar curse words were used, and the targets were called names. Again, a classic flame. However, there were differences. The mail was not sent to a group, but directly to individuals who had been chosen because of their race. In addition, the email made direct death threats. Not of the general "You should die" variety, but specific "I will hunt you down and kill you." At the trial, the defense for Machado made a point of emphasizing the flame like nature of the email, while the prosecution pointed out the direct, targeted

threats. This argument became so central that newspaper reporting on the trial began to talk about the "flame defense."

This case can certainly motivate a discussion of online behavior and the appropriate rules for it. But it also shows the difficulty people (like Machado) have with the boundaries between different cultures. What looks like a fine, and even funny, flame in one context can look like a serious offense in another. The electronic world does not make it easy for people to make these distinctions on their computer screens.

The context of U.C. Irvine and the surrounding community

If you read the perspectives document on Machado and on the UCI community, you will begin to see some of the underlying racial tension that exploded with Machado's email. The Hispanic population in California had been rapidly increasing, while their admission to university had hardly changed from its already low level (and in some places gone down). On the other hand, Asians were far over-represented in California universities given their percentage of the California population. This is another example of a culture clash occurring in this case. Machado felt the over-representation of Asians at UCI was unjust.

UCI, like most other universities, tried to create a climate in which people could discuss ideas, even if they were unpopular. Thus, UCI was committed to the value of free speech. But Machado's speech crossed the line when, instead of being simply racist, he threatened specific Asians with death. Most universities do not encourage racist speech among students, though some tolerate it because they value free speech. Officials at universities use the word toleration carefully. Behavior is tolerated if it is allowed but disapproved of.

Machado felt like he had a tremendous amount of pressure on him to succeed for his family, but that both circumstances (his brother's murder) and the university system (his low grades) were conspiring against him. There was reasonably convincing evidence presented at the trial that Machado was clinically depressed at the time he made his two hate mailings.

It is easy to think that Machado should have sympathized with the Asians rather than threatening them. But to do this is to fall prey to the "model minority" myth. Minorities are thought of as greater failures than majority members if they express racist ideas or otherwise show anger and resentment. Suffering usually does not make people noble.

Law enforcement

Part of Machado's problem was that his case came along at the wrong time -- or, for the FBI, at just the right time. No one had yet shown that hate mail sent over email counted as illegal. The FBI needed a case to prove this, and Machado was the lucky trial case.

The accused in a previous case in Michigan (United States v. Baker, 1995) had been acquitted of threatening rape over electronic media (with a "fictional" story that used the victim's real name). But Machado's email seemed like it could pass muster because of its specificity.

It was still a tough case to try, and the first attempt ended up in a mistrial because the jury was hung favoring acquittal. But additional evidence about Machado's attitude and habits turned the tide in the second trial.

Here we come up against another culture clash in the socio-technical system, this time between the legal system and university culture. The primary job of universities is to establish a climate in which students can be educated. Thus, tolerance and care for the individual are emphasized. Almost all electronic mail offenders are dealt with in-house at universities. UCI has even established a sort of "traffic school" for those who break the rules. This both confronts the offender with clear evidence of the wrongdoing and provides a supportive way for people to learn to do better.

But the culture changes when you enter the legal system. Here primary goals are enforcing the law and careful establishing and following of procedures to assure justice is done. The Machado case was a chance to establish a precedent of email as a medium for hate crime. Thus, finding Machado guilty provided not only justice in the case (from the perspective of the prosecutor) but also put the case (and the prosecutor) on the map of legal precedent. The only responsibility to Machado was to try the case fairly.

Ethical Reflections

Competing Values and the ImpactCS Grid for Machado

If we use the framework from chapter 2 to analyze the Machado case it certainly highlights some important issues in almost every column of ethical issues defined by the framework. In addition, some of these issues need to be addressed as more than simple individual ethical decisions about whether to send hate mail or not; we will need to look to the group, national, and global issues involved.

If the theme of the socio-technical analysis for this case was clashing cultures, a reasonable theme for the ethical analysis is about competing values. Does Machado's right to free speech override the right student's have to a safe environment to go to school? Do individuals' right to privacy override the need of those running a network to track down people using electronic methods (including surveillance)?

Sticking with values

Notice first how the language moves quickly back and forth between rights and values. We can usually describe some right an individual has as being based in some thing we value (e.g. the right to privacy is based in the value we place on autonomy). You can see how this is done in chapter 12.

There is another reason to be clear about the values or social goods associated with rights: it helps people keep a more open mind. Rights are often talked about as though they were absolute and inviolable. "I have an unconditional right to privacy and to freedom of speech." But the right to freedom of speech can get in the way of the right to privacy, and if they both will not budge, then our discussion stops. If we move instead to saying we value each of these things, then we can ask how much we value it, and how we balance it against other, competing values.

Quality of Life

Certainly the individuals who designed the "finger" command and its network protocol did not intend for the command to be used to single out, for harassment, people with certain ethnic names. The purpose of these commands was to find out information about people in a collaborative atmosphere. Given its wide availability, it seems reasonable to think that it has succeeded in enhancing the online quality of life by helping people to find each other.

The email transfer protocol, SMTP, has also been a success. The time stamps initially designed to track the efficiency of the email transfer process have been used for different purposes, many of them ones that receive wide approval. For instance, time stamp headers are used in tracking down the originators of unsolicited commercial email (commonly known as "spam"). In our case the headers were used to track down the originator of hate mail. There are a variety of other uses for these headers.

Thus a software tool (like SMTP or finger) can be reused for both bad and good purposes. We cannot expect the designers of tools to foresee all (or even most) of these reuses. But we might expect designers to design knowing that some reuse will be done.

Use of Power

There really are two uses of power in this case that require some ethical inquiry, though both of them might be obscured by other issues at first. They both have to do with the use of power, in one case by computer professionals and in the other by users. We can think of the duties of computer professionals in this case under two categories: their duties as employees and their duties as computer professionals.

Use of power by employees

One way of analyzing the issues at stake is simply to think of Dana Rood and Allen Schiano in their roles of employees of the University of California, Irvine. They are hired by the university to maintain a computer system for the use of students, faculty, and staff at the university. If we use the analysis approach proposed by Collins and Miller [3] we should ask "to whom do these people owe duties?" For the sake of simplicity, let's talk about two of these sets of duties:

Duties to their employer. Certainly they owe it to their employers to implement and configure an efficient, reliable, and current computing system, within the limits of their budget and time. In addition, they have a duty to their employer to keep them safe from losses due to lawsuits, harmful software, and other harmful actions that might be foreseeable by the computer professional.

Duties to their users. They have some similar duties to users, in that users expect a reliable and reasonably current computer system. But users also expect a safe computer system (an environment in which they feel safe) and they have at least an expectation of reasonable privacy.

The privacy of electronic mail is a tangled topic, and you should see the discussion on privacy for an initial discussion of it. However, considering the duties of Dana Rood and Allen Schiano simply as employees presents an interesting difficulty: There may be situations in which one’s duties to the employer conflict with one’s duties to the users (the Therac-25 case may have been one of these). In some companies, computer professionals have been asked to implement detailed employee performance tracking and surveillance systems. In these cases, some individuals have felt their duties to be in conflict.

But are Rood & Schiano’s duties really in conflict here? In fact, their duties to their employer and their duties to their users (particularly the Asian students who were targeted) converge. So, simply as employees of the college and as service providers to the students, Rood and Schiano have a duty to protect students from harassment and from invasions of their privacy.

It would be rash to assume, however, that these duties will always agree so easily. It would be equally rash to assume that, in the case of a conflict, one set of duties always trumps the other.

Use of power by computer professionals

In addition to being employees, Rood and Schiano are also computer professionals. They have special expertise in computing that qualifies them to make decisions about computer systems. The question about whether computing is a profession is a complex one. Deborah Johnson [7] provides an initial discussion motivated by the ethical implications of professional status, and Pavalko [1] provides a more sociological look at the issue.

But for the sake of this discussion, let's assume that the special expertise that Rood and Schiano have comes with some additional responsibility. Why would this be? To the extent that special expertise allows a person to foresee the results of an action better (e.g. a meteorologist and the weather, a doctor and a prescription) that special expertise imposes an additional responsibility to avoid harm given that it is (or should have been) foreseen.

As an example, review the discussion in the socio-technical system section on the finger command. This command makes available personal information about users to those who invoke the command. Early RFCs for implementation of this command, even on networked systems, made no mention of the privacy or safety issues that might be associated with the widespread availability of this capability. Is there anything inherently wrong with providing this capability? Well, we can certainly think of cases where this capability would be nice to have, and even an addition to the quality of life of individuals who had access to the command. So, there is probably nothing inherently wrong with the idea. But later RFCs for finger protocols do contain clear discussion about the privacy implications of the command.

Decisions about whether or not to implement and how to configure a finger server are usually made by computer professionals. These computer professionals have this responsibility because of their technical expertise and because of the role they occupy in an organization, usually that of director or manager of systems.

In our case, we may have a situation where the harm from implementing the finger command was not foreseeable until the potential for harm was pointed out by our culprit, Mr. Machado. At a more general level, computer professionals who design or implement systems may find those systems being used in ways they could not have foreseen, and may not agree with. But their design or implementation may still contribute to the problem.

Huff [5] calls this ability of computer professionals to affect others by the systems they design or implement, unintentional power. In these cases, the question is whether a reasonable person with that expertise should have foreseen the harm. Some RFCs occurrences prior to the Machado case did point out the possibility of privacy violations. But it was still standard practice at that time to implement a finger server on university

computing systems. It is still standard practice to do so today, at least for queries done on the campus.

Use of power by computer users

Machado clearly used the added power that computing gave him to harass and intimidate Asian students at the university. Given Machado's defense in court (and his failing grades, expulsion, etc.), he probably felt like he had very little power on campus. But the computer gave him power to speak to people he did not know, and whom he held indirectly responsible for his plight: Asian students.

Again, the issue of the foreseeability of the consequences comes into play here. And the question is not whether Machado could foresee the harm his email might do (he said he did not think it would do harm). The issue is whether a reasonable person would foresee the harm. Determining what we mean by "reasonable person" in this case is one of the things at issue. Comments made at trial by the defense suggested that people on a networked system reading email might expect "flames" and that, given that assumption about the nature of electronic communication, any harm that did occur was not foreseeable by someone familiar with that online culture. In the end, the jury did not agree with this analysis. But whether the jury was right or not is still open to discussion. To begin thinking about this issue, you might read the section on socio-technical analysis for this case.

So, the use of power in the ImpactCS framework is not just about the use of power that comes with special expertise in computing, but also encompasses the use of the power that computing technology gives individuals.

Safety

Clearly there were threats to the safety of individuals in this case. Machado probably was not going to "hunt down and kill" the Asians he sent email to, but they could not know that, and some of the targets reasonably felt their safety threatened. How does this relate to computing ethics? How did Machado find out the names of the individuals? By making the email addresses of individuals easily available through a finger server, the OAC contributed in some way to Machado's action.

How should computer professionals think through this issue when setting up networked systems? One question that an operator of a system needs to ask in this case is: how do the benefits of providing this information online balance the dangers to which it might contribute? This cost/benefit analysis is not an easy one, but it is important.

Equity and Access

The question on which the criminal trial of Machado hung was whether, by sending his emailed threats to the particular individuals he had targeted, he had interfered with their civil rights to access to public education. The jury and the court in his case answered "yes." They concluded that the fact that the email was specifically targeted at particular individuals, that it contained death threats that were at least credible, and that the intent of

the email was to tell the Asians to stay away from the university, that Machado had indeed interfered with their civil rights.

But this issue, as interesting as it is, gets us away from specifically computing related ethical issues. It does leave us with an interesting social issue: why would people (particularly Machado) think that a thing that is illegal or immoral when done face-to-face or with unsigned letters in mailboxes would become acceptable (or at least tolerable) when done over email? And with this issue, we go back to the socio-technical analysis theme of a clash of cultures. In essence, Machado confused the cultural norms that were at least tolerable on some Internet newsgroups with what would be tolerated in direct mail to targeted individuals.

An ethical issue that this raises for designers of communications software is how they might make the context in which a person is sending a message more salient to the user. If it were more clear who the audience was for a particular communication, it might make it easier for individuals to adapt their communication to the rules of the community they were addressing.

Would this have helped in the Machado case? Likely not. But it might help in other instances, and seems worth exploring.

Free speech

As the Supreme Court has made clear in its Brandenburg decision (see Legal Climate in the resources section) the right to free speech needs to be balanced with other rights. There is a history of devotion to free and unfettered speech among computing professionals, and on Internet newsgroups and other forums. But few would argue that this right can never be trumped by another right. It would be more helpful to ask "What values conflict at times with free speech?" Certainly speech that threatens the safety of others conflicts with our value for life and privacy.

Was the University obligated, because of its educational position as a forum for free speech, to provide Machado with a forum to express his views? Most college and universities think of themselves as valuing and encouraging free speech and open inquiry as a part of the academic enterprise. But personal electronic mail is not really "public" speech. The proliferation of electronic mail lists for discussion helps to confuse this issue somewhat. However, Machado was not using a mailing list -- he was sending electronic mail to particular individuals. Would (or should) Machado's speech be more protected as "free speech" if it were done in a different forum?

Moving to the global level of analysis, in other countries many other values would be considered important enough to conflict with the right to free speech. In Canada and Britain some trials are closed to public reporting, because the concern that individuals receive a fair trial is valued more than newspapers' freedom to report on the trial. In Germany, pro-Nazi speech is unconstitutional. In other countries, any political speech that criticizes the government is viewed as too dangerous to be allowed. Often (though certainly not always) these policies restricting free speech have popular support.

But again, we are straying somewhat far from the Machado case. We can at least note that in some countries (and in our country before the passage of the Civil Rights Act) what Machado did would not be considered illegal. We may still ask whether it would be moral.