The "Memogate" Affair: A Case Study on Privacy in Computer Networks

Edward F. Gehringer
North Carolina State University
efg@ncsu.edu

Abstract

Privacy is one of the core issues in any Ethics in Computing course. It is important for system administrators to keep sensitive data private, but suppose they don't? Then what are the obligations of someone who accidentally gains access to this data? This is the crux of the issue in last year's "Memogate" case involving the Senate Judiciary Committee. Files on the Judiciary computer system were mistakenly left unprotected. This allowed Manuel Miranda, a staffer in the office of Judiciary Committee Chairman Bill Frist, to view confidential memos written by Democrats on the committee. These documents revealed political maneuvering and some actions that were arguably unethical. Miranda was fired by Frist, but engaged in a spirited defense of his actions in the media. The legalities of this behavior are in dispute, with prosecution being a possibility. This case raises several ethical questions, including, How much of an obligation does one have to avoid viewing the private information of others? Does it depend on whether the administrator knew the documents were unprotected, and did nothing to "fix" it? Can this obligation be outweighed by an obligation to expose (other) unethical activity? To what extent is this action similar to a student viewing someone else's unprotected computer code and then submitting it as his/her own work? Or suppose the student just viewed it, but did not submit it; would that still be unethical? This case can serve as interesting, current, case study in privacy rights in a computer network.

1. Introduction

The ACM/IEEE-CS Computing Curricula 2001 [1], in its Social and Professional issues area, lists seven "core" units that should be a part of any curriculum. Unit SP7 is "Privacy and civil liberties." Students need to understand the importance of placing appropriate access restrictions on sensitive information, and of not breaching the confidentiality of private information that might come into their possession. An effective method of instilling understanding is the case-study approach, in which students are presented with real-world examples of dilemmas that they might encounter, and challenged to apply ethical principles in deciding on a proper course of action.

A good case study has several attributes. It should require students to evaluate competing objectives (e.g., the interests of one's employer vs. the interests of society). It should be realistic—something that could actually happen, or has happened. It should pose ethical challenges that are distinct from whatever legal issues are involved; after all, we are teaching ethics and not law. It should provoke spirited discussion; often the best cases are ones that are controversial, where students might reasonably take opposing sides.

The "Memogate" case from the (U.S.) Senate Judiciary Committee in 2004 seems to have all of these attributes. The basic question is strikingly simple: Is it ethical to read and disclose the contents of other users' unprotected computer files? Should the answer be a clear "yes" or "no",

or does it depend on the circumstances? For some insight, let's examine the facts of the case.

2. "Memogate": The Facts of the Case

In late 2001, Jason Lundell, a nominations clerk for the Senate Judiciary Committee, found out that he could access files [2] belonging to both Republicans and Democrats on the committee. According to one account [3], he discovered this simply by doing a search for "Judge Charles Pickering," who had been nominated by President Bush for a seat on the Fifth Circuit Court of Appeals, and was being opposed by Democrats. Another report [2] says he made this discovery after watching the Committee's system administrator "perform some work on his computer." This did not require any special access rights; any user could do this simply by clicking on "My Network Places>Entire Network>Judak." This publicly readable area contained files with committee schedules, hearing minutes, and memos on the Democrats' strategies for blocking the controversial nominations. It was unprotected due to an apparent mistake by the new system administrator hired when Democrats took control of the Senate in May 2001. He set the default permission on new directories to be "public," even though they were supposed to be password-protected [4, 5].

While Lundell was the one who discovered the vulnerability and accessed most of the files, the central figure in the case became Manuel Miranda, who was a counsel to Senate Majority Leader Bill Frist. Over an 18-month period, he used information on dates and times of nomination hearings to prepare defenses for the nominees. He was also suspected of leaking the memos to the *Wall Street Journal* [6], which used them to write a Nov. 14, 2003 editorial accusing the Democrats of misconduct. When the extent of his activities was revealed, Miranda was fired by Senator Frist [2].

3. The Ethics, Take 1

Prima facie, Miranda and Lundell's actions were unethical because they violated confidentiality. Senate Judiciary Committee Chairman Orrin Hatch put it like this, "I am mortified that this improper, unethical and simply unacceptable breach of confidential files occurred. … There is no excuse to justify these improper actions. None of us would walk into another person's office and take papers from their desk, and this is, in a sense, exactly that" [7]. Senator Ted Kennedy compared it to Watergate: "In those days, break-ins required a physical presence, burglar's tools, lookouts and getaway cars. Today, theft may only require a computer and the skills to use it and the will to break in" [8].

The analogy seems compelling. Reading unprotected files on a computer is a lot like taking documents from an empty unlocked office. The two actions are not exactly the same, because after documents are physically removed, the owner can no longer read them. The interloper may copy and return them to escape detection, but that would not obviate the ethical violation. In the Watergate break-in, the burglars were not intending to deprive the Democrats of any of their documents, just to scan them for embarrassing or incriminating information. Miranda's motivation was similar. Of course, he did not actually break in, but as Hatch's comment illustrates, that may be irrelevant. Burglary is still burglary, even if the door is unlocked.

One test of the ethics of an action is whether it is *universalizable*—that is, if society could function if everyone acted that way. Consider the implications for the private sector. Many employees use shared networks that contain a plethora of confidential documents—everything from corporate strategy to trade secrets [9]. Can you imagine the animosity and legal wrangling that would ensue if the average corporate employee behaved the same way?

Most people would agree that hacking by password-guessing is unethical. People employ weak passwords (e.g., words from the dictionary) even though they are warned not to. Can one claim that it is OK to snoop through accounts with obvious passwords? If the answer is no, then can it be ethical to look through files that are accidentally unprotected?

The District of Columbia Bar deems it unethical for a lawyer in an adversary proceeding to use a document that may have been stolen or taken without authorization from an opposing party [10]. However, Miranda argued that a Senate confirmation hearing is not "an adversary proceeding" [11].

Ethical, of course, is not the same thing as legal. Nevertheless, the law is a good indication of what Congress considers ethical. Federal law prohibits "having knowingly accessed a computer without authorization or exceeding authorized access." It is also against the law if someone "embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record" [8].

4. In Defense of Miranda

After his dismissal, Miranda mounted a spirited defense of his actions in op-ed pieces and on talk shows. His defense rested on two main points: that he was fully authorized to view and disclose the documents in question, and that being a whistleblower requires disclosure of material not intended for public view. Let us examine each of these.

As to Miranda's right to access the documents, argued his lawyer Arthur McKey, a computer-law expert, "The Democrat-controlled 'server' quite literally gave … Mr. Miranda the unprotected documents. … Under the law and practice, there can be no doubt that every authorized [Judiciary Committee] user had an affirmative grant of access and were entitled to read any unprotected document on the [Judiciary] server" [11] In arguing that Miranda's actions were unethical, we used the analogy of walking into an unoccupied and unlocked office. Miranda, however, claimed that giving him desktop access to the server was "like putting the documents on our desks …" [9].

We might agree that disclosing the information was wrong only if it was "confidential" in some sense. Disclosure of confidential documents is prohibited by Senate Rule 29.5 [12]. Miranda's lawyer argues that after the brouhaha over Anita Hill's charges at the Clarence Thomas confirmation hearings, the rule was clarified to cover only Senate "business proceedings," such as official committee business or FBI files, not staff memos [13]. So, under the meaning of the rule, the documents disclosed by Miranda were not "confidential."

If there is any wrongdoing in the disclosure of the information, Miranda's defenders argue, it

rests with the system administrators who left it unprotected in the first place. "The Economic Espionage Act requires information to be protected to the same extent that one seeks to classify it as a secret or claim legal protection," writes Ira Winkler [14]. In fact, if confidential information was left unprotected in "public or healthcare-related" corporations, corporate officials could be heavily fined or incarcerated, under the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, or the Gramm-Leach-Bliley Act.

Miranda's second point is that in revealing the Democrats' strategy, he was acting as a "whistleblower" by revealing conduct that was unethical or illegal. He was entitled, indeed, obligated to do this by the Code of Ethics for Government Service, which requires government employees to "expose corruption wherever discovered." Setting aside, for now, the question of whether the conduct in question was actually wrong, it seems self-evident that few wrongdoers would document their sins in media intended for wide distribution. So, sometimes it is necessary to reveal information not intended for public consumption. How else would corruption be discovered [15]?

Following this reasoning, in order to determine whether Miranda acted unethically, we need to examine his claims about the ethics of the Democrats' actions. These claims are, of course, outside the scope of an Ethics in Computing course, but they are typical of charges and countercharges in a political environment (government or corporate), and so it is worth at least recounting them.

Most serious is the charge that Senate Democrats postponed the confirmation hearing of Judge Julia Gibbons for the Sixth Circuit Court of Appeals in order to influence the outcome of the affirmative-action case against the University of Michigan. It is based on a request by Elaine Jones, then-president of the NAACP Legal Defense Fund to Senator Kennedy's staff that the vote be delayed. This could easily be "an attempt by an interested party to influence a tribunal" [16], and there is a good case that it changed the outcome of the case, decided by a 5–4 vote of the court. It led to an ethics complaint against Jones before the Virginia bar. But, this was not wrongdoing by anyone associated with the committee or the US government, so going public with the charge might be more akin to politicking than whistleblowing.

Another charge is that Senator John Edwards asked then-Chairman Senator Patrick Leahy to delay the vote on another nominee to protect campaign contributions. Federal law prohibits Senators from accepting money, gifts, or promises of support in direct exchange for votes. But in this case, no evidence of a direct swap has yet been adduced [16]. The Democrats, in their memos, referred to judicial nominee Miguel Estrada as particularly dangerous because he was Latino, and would therefore attract sympathy that would make him difficult to block from a higher federal judgeship. The Committee for a Fair Judiciary argues that this constitutes racial discrimination in hiring, and is therefore criminal. Maybe so, but the standard for conviction is proof beyond a reasonable doubt, and as everyone knows, racial and gender characteristics often play a major role in political appointments.

In any event, whistleblowers are often advised to "go public" only if internal efforts to resolve the problem prove unsuccessful. This suggests that Miranda should have filed a complaint with the Senate Ethics Committee before going to the media.

5. The Broader Context

Returning to the basic question, Is it legitimate to view and disclose the contents of files which one is authorized to access? let us consider diverse cases that seem to raise the same issue.

First, a federal court has found that obtaining access to a password-protected Web site by using another person's password is a violation of the Computer Fraud and Abuse Act, even if the other person has voluntarily given the password away. The case of IMS vs. Berkshire [17] involved one software company gaining access to another company's site through a password given to them by a customer of the other company. They were then able to reverse-engineer the first company's sorting algorithms in their own magazine-tracking service. This is similar to the Memogate case in the sense that it involves the *authorized* access of information to which one was not *supposed to* have access.

There are many cases in which accidentally-revealed information has influenced society. Most prominent in the past year was the case of vote-counting software from Diebold, Inc., a manufacturer of electronic voting machines. In January 2003, someone accidentally placed the code on a publicly accessible Internet server [18]. The code was subsequently analyzed by four respected computer-security researchers, led by Avi Rubin of Johns Hopkins University. They concluded [19] that a voter could shut down the machine before the polls officially closed, or a poll worker could deliberately cause votes to be miscounted. Diebold denied the plausibility of these scenarios, saying that many of them "only apply if the voting terminals are connected to the Internet or some other public network. This is never the case."

Was it ethical for Rubin et al. to perform this research? They were, after all, working with code that Diebold did not intend to reveal to them. Clearly, the disclosure was not in Diebold's interest, but it ostensibly benefited the American public because it fueled the high-profile debate over the reliability of electronic voting and the perceived need for some sort of audit trail so that the count can be checked. It has undoubtedly also led to greater attention to testing and verification by the manufacturers of these devices. Thus, it seems too sweeping to say that it is always unethical to read or disclose information to which one accidentally has access.

An even more recent example, also related to voting, is the inaccuracy of exit polls in the 2004 Presidential election. Most major news organizations pulled the polls from their Web sites once the vote began to go the other way, but CNN, through a "computer glitch," left theirs up until 1:30 AM election night. This provided data for University of Pennsylvania faculty member Steven Freeman to analyze [20]. He reports that no other news organization would honor his request for exit-poll data. Although others question his conclusions [21], would the nation really be better off if this research had not been done?

In other contexts, it seems less ethical to use accidentally acquired information. Suppose you are a student working on a programming assignment, and another student leaves his code in an unprotected directory; is it OK for you to use it in your own program? Clearly not; that would be plagiarism. But suppose you just *read* his code to figure out how to write the program? Is that OK? The answer is not so obvious in this case, but it is still no. The reason is that it is not universalizable; if everyone were able to read everyone else's code, it would be impossible to prevent some students from using the code in their own submissions. Indeed, students frequently

give others access to their code "just so they can read it and learn," and then find that they have submitted it as their own [22]. One might argue that programs such as Moss [23] can prevent this form of cheating. But that is true only if cheating occurs among small groups of students. In a situation where everyone's code was public, it would be very difficult indeed to discern who was the real author.

6. Final remarks

There seems to be no clear answer to whether using information to which one accidentally has access is *always* unethical. Thus, we need to consider the circumstances more closely. Let's return to the Memogate case.

The first circumstance is the time period over which the accesses took place. The Senate Sergeant at Arms determined that Miranda had viewed the documents over a period of two years, and saw more than 5000 documents [16]. This doesn't sound like the Diebold or CNN cases, but rather like a "long-term political spying operation" [24]. Miranda says that in the summer of 2002, the Republicans' computer technician told his Democratic counterpart of the misconfiguration, but the Democrats did nothing to fix the problem [4]. Should Miranda have warned them again? Should the whistle have been blown on the careless administrator a year before the most politically charged memos were leaked?

Another difference from Diebold and CNN is that those were cases where an unaffiliated person was able to access documents on an outside server. One probably owes one's own colleagues more deference and trust than one owes to an outside party. Members of a single organization need to be working as a team, and this suggests that surreptitiously accessing documents of one's colleagues is worse than purloining documents from another organization. This line of argument must be tempered against background of negative ads that Senate "colleagues" perennially run against each other. But it is still true that between elections, the business of governing must be done.

Detractors of Miranda say that there was no negligence on the part of the Democrats; no one knew about the open access, and they had every reason to believe their files were secure [25]. It is true that very few people admitted knowledge of the access glitch. However, this may have been because an unnamed Judiciary Committee member warned them that "anyone admitted they knew how to access the open server would be fired" [26].

Another question is whether Miranda's actions placed his own compatriots at risk. If knowledge of the access hole was widespread, it was quite possible that Democrats were reading Republican memos. Wouldn't he have had an obligation to tell his own bosses of the problem [25]?

This case seems ideal for discussion in a computer-ethics class, since it is current and very easy to explain, but quite challenging to analyze. There are implications for their own actions as students, and in their future employment. I have found that my students can defend diverse viewpoints on this issue. It is a good vehicle for teaching ethical reasoning.

Bibliography

[1] Association for Computing Machinery and IEEE Computer Society, *Computing Curricula 2001*, http://www.computer.org/education/cc2001/final/

[2] John M. Powers, "Hatch and Frist fire whistle-blower," *Insight on the News*, April 26, 2004, p. 24.

[3] Gail Russell Chaddock, "'Memogate' opens window on judiciary fights," *Christian Science Monitor*, March 17, 2004, p. 2

[4] Charlie Savage, "Infiltration of files seen as extensive," *Boston Globe*, January 22, 2004, http://www.boston.com/news/nation/articles/2004/01/22/infiltration_of_files_seen_as_extensive/

[5] Christopher Hayes, "Watergate Redux: Calls mount for investigation into Republican staffers' piracy of Democratic files," *In These Times*, March 13, 2004, http://www.inthesetimes.com/site/main/article/watergate_redux/

[6] Paul Kane, "Judiciary report unveiled today," *Roll Call*, March 1, 2004.

[7] Cnn.com, "Leahy: Justice department to probe leaked files," April 26, 2004.

[8] Jesse L. Holland, "Judiciary Committee memo snooping, investigation stirs uproar," Associated Press, Feb. 13, 2004.

[9] Robert Varmosi, "Why hacking the U.S. Senate is apparently A-OK," c|net, January 28, 2004, http://reviews.cnet.com/4520-3513_7-5118858-1.html

[10] District of Columbia Bar, "Opinion 318: Disclosure of Privileged Material by Third Party," http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion318.cfm

[11] Jonathan Groner, "Miranda warning: Hardball on the Hill," *Legal Times*, March 31, 2004, http://www.law.com/jsp/article.jsp?id=1080334960393

[12] Standing Rules of the Senate: Rule 29, Executive Sessions, http://rules.senate.gov/senaterules/rule29.htm

[13] Arthur D. McKey, "Re: Legal response to the Pickle report," www.cfif.org/htdocs/legislative_issues/federal_issues/ hot_issues_in_congress/confirmation_watch/mckey.pdf

[14] Ira Winkler, "Memo Gateless," *National Review Online*, March 4, 2004, http://www.nationalreview.com/comment/winkler200403041011.asp

[15] Manuel Miranda, "What wrongdoing?" *National Review Online*, March 11, 2004, http://www.nationalreview.com/comment/miranda200403111041.asp

[16] Dahlia Lithwick, "Memogate," *Slate*, Feb. 19, 2004.

[17] Joe Metcalfe, "District court concludes that obtaining access to a password-protected Website using another person' s password is a violation of the Computer Fraud and Abuse Act," http://hermes.circ.gwu.edu/cgi-bin/wa?A2=ind0403&L=cybercrime&F=&S=&P=70 Refers to IMS Inquiry Management Systems v. Berkshire Information Systems, F. Supp. 2d, 2004 WL 345556 (SDNY, Feb. 23, 2004)

[18] Paul Boutin, "Hack the vote: How to stop someone from stealing the 2004 election," *Slate*, July 31, 2003, http://slate.msn.com/id/2086455

[19] Steven M. Cherry, "Security experts question leading e-voting system," *IEEE Spectrum Online*, July 30, 2003, http://www.spectrum.ieee.org/WEBONLY/wonews/aug03/evoting.html

[20] Steven F. Freeman, "The unexplained exit poll discrepancy," truthout.org/unexplainedexitpoll.pdf

[21] John Allen Paulos, *Philadelphia Inquirer*, November 24, 2004, http://www.math.temple.edu/~paulos/exit.html

[22] Zelna, Carrie Lynn, "Academic integrity and the Internet," Ph.D. dissertation, North Carolina State University, 2002, p. 89.

[23] Moss: A system for detecting software plagiarism, http://www.cs.berkeley.edu/~aiken/moss.html

[24] *Washington Post*, "Anything doesn't go," Editorial, March 7, 2004, p. B6.

[25] Kevin Drum, "Political animal," *Washington Monthly*, March 9, 2004, http://www.washingtonmonthly.com/archives/individual/2004_03/003445.php

[26] Alexander Bolton, "Miranda files rebuttal to memo report," *The Hill*, March 11, 2004.

EDWARD F. GEHRINGER
Edward Gehringer is an associate professor in the Department of Electrical and Computer Engineering and the Department of Computer Science at North Carolina State University. He has been a frequent presenter at education-based workshops in the areas of computer architecture and object-oriented systems. His research interests include architectural support for persistence and large object systems, memory management and memory-management visualization, and garbage collection. He received a B.S. from the University of Detroit(-Mercy) in 1972, a B.A. from Wayne State University, also in 1972, and the Ph.D. from Purdue University in 1979.