AC 2009-1719: PERSONAL VS. PROFESSIONAL E-MAIL: THE PALIN CASE

Edward Gehringer, North Carolina State University

Ed Gehringer is an associate professor in the Department of Computer Science and the Department of Electrical and Computer Engineering 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 memory management, garbage collection, and computer-supported collaborative learning. 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.

Personal vs. Professional E-mail: the Palin Case

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

Abstract

Last fall's break-in of Vice-Presidential candidate Sarah Palin's private e-mail account can serve as a fascinating case study in an Ethics in Computing class. The break-in is a clear violation of federal law, and the ethics of that should not be in serious doubt. But what about posting the contents of her private e-mail on a public Web site? Was that unethical too, as a violation of privacy? Suppose the information posted revealed an indiscretion relevant to the campaign or a violation of the law, would it still be unethical, or does the public have a right to know? The Diebold case from a few years ago comes to mind; here confidential information about e-voting software was posted accidentally and resulted in a much-needed security audit. And what of the claim that Governor Palin was conducting some state business using her Yahoo account? If she did this to circumvent state open-records laws, it would clearly be illegal; but if not, could it still be considered unprofessional? And if so, is *all* business use of unofficial e-mail accounts unethical, even if the purpose is to, e.g., accommodate larger attachments than inboxes can hold on the employer's e-mail system? Suppose the employer has a policy (as some universities do) of allowing private use of the employer's computer equipment, as long as it does not hinder official use? How can our students protect their accounts against break-ins? Not only does this case raise important privacy issues, it also touches on the issue of separation of work and personal life, which all of our students will face as they begin their careers.

1. Introduction

When someone, allegedly David Kernell [1], hacked into Vice-Presidential candidate Sarah Palin's Yahoo account [2] last September 16, he highlighted a distinction that is rapidly growing in importance in today's social-networked world: the difference between personal and professional e-mail. A decade ago, the average person might have had a single e-mail account. But now, increased monitoring by employers has led most employees to separate their "home" and "work" e-mail accounts. While the author could find no ethical guidelines that would *require* such a separation, it is clear that some activities should not go on using work e-mail while others are inappropriate on personal e-mail.

2. Personal use of professional e-mail accounts

Many employers permit personal use of company e-mail accounts, treating it the same way that they treat personal use of the telephone—it's OK as long as it doesn't get in the way of work activities. But that, obviously, does not include exchange of pornography, and companies also fire employees for offensive language and e-mail harassment. In fact, an American Management Association survey showed that about two-thirds of companies monitor their employees' e-mail, and more than a quarter of companies have fired employees for misuse of their e-mail [3]. And e-mail is not quite like the telephone, because every outgoing message bears the name of the

employer [4]. This suggests caution in the use of professional e-mail for personal purposes.

For an employee of a government entity, including state universities, there is an additional reason to be careful: Any e-mail sent to a government employee is a public record [5], and open-records laws may allow any member of the public to obtain the contents of specific messages [6]. While this rarely happens, it is conceivable that any newsworthy e-mail sent to a government employee could wind up in the newspaper. It is simply safer to route personal messages through personal e-mail accounts.

3. Professional use of personal e-mail accounts

Conversely, an employee needs to be cautious about using personal e-mail for work communication. Personal e-mail doesn't carry the footer added by many companies that says it is only for the use of the recipient to whom it is directed. Thus, the employer has less legal protection against misuse of the message by third parties.

Under the Electronic Communications Privacy Act of 1986, e-mail sent over public networks such as Yahoo or AOL is private. Thus, it is problematical to conduct government business through these services, since open-records laws require such communications to be accessible to the public [6]. Using private channels to conduct such communication is a violation of the law.

Indeed, this was the reason for the complaint against Palin's use of Yahoo e-mail [7, 8]]. Critics charged that she used it in order to prevent the messages from being subpoenaed [9]. Press reports do not make it clear how much state business was in fact conducted on the Yahoo accounts. Several reports say e-mails were posted on the Web with subject lines such as, "Draft letter to Governor Schwarzenegger/Container tax" and "DPS Personnel and Budget Issues" [10]. However, the bodies of those messages are no longer posted. What can be found are messages that are personal (e.g., encouraging words from a friend) [9] and political [11, 12] (e.g., discussions with Lieutenant Governor Sean Parnell during his primary campaign for Congress). Political use of state resources (e.g., an official e-mail account) would be illegal.

This was not the first time that Palin's use of personal e-mail accounts had come under scrutiny. An Anchorage "watchdog" named Andrée McLeod had filed a request for 1100 e-mail messages that he said related to policy deliberations [13]. He questioned whether Palin was using private e-mail to evade the public-records law [14].

Palin was not the only governor who has used private e-mail accounts. In his first two years in office, Iowa Governor Chet Culver rarely used his government e-mail account, preferring to use a private server instead [15]. But after the Associated Press began looking into the practice, aides said he had begun using his state e-mail account. Others have gotten into hot water for deleting e-mail. Former Missouri Governor Matt Blunt had a practice of deleting e-mail [15]. Aides to Texas Governor Rick Perry had been deleting official e-mail after seven days. This is potentially a serious problem, since deleting records that may be needed in an investigation is illegal [16].

4. Three ethical issues raised by this case

This case touches issues such as illegal access, privacy, and security, all of which are important to students in computing sciences and engineering. The most obvious is *illegal access*. Breaking into the account is a clear violation of the Computer Fraud and Abuse Act. Kernell was charged with violating this act by "knowingly accessing a protected computer with the intent to defraud." While there is doubt over whether he should have been charged with a felony for doing so [17], there is no doubt that the perpetrator broke the law. Unfortunately for him, being involved in a high-profile break-in increases the motivation for the government to mete out severe penalties. Kernell has now been charged with three additional felonies [18]: identity theft for impersonating Palin, obstruction of justice for deleting evidence (the e-mails and screenshots) from his laptop, and wire fraud for posting stolen information to the Internet. Fearing that use of the term "hacker" might prejudice jurors against him, Kernell's lawyer filed a motion to prevent prosecutors and witnesses from referring to him as a "hacker"—a term they said refers to someone with "specialized computer skills" who damages information in a computer [19].

Similarly, there can be little question that the posting of personal e-mail on the Web is a violation of the sender's *privacy* [20], even if the sender is a public figure. In this case, the gossip site Gawker obtained the cellphone number of Palin's daughter Bristol, and posted her voicemail response on the Web. They posted the e-mail addresses of Palin's husband and son. This would be an invasion of privacy even if the personal e-mail revealed an indiscretion that was newsworthy during the campaign. But what about posting professional e-mail sent from a personal account? Such e-mail was supposed to be available to the public anyway. However, it does not seem ethical for a private individual—in fact, one who has just broken the law by accessing the information—to make a decision that should be made by a court of law.

Superficially, this case seems similar to the Diebold case [21], where code for an e-voting system was accidentally posted on the Internet and subsequently analyzed by computer scientist Avi Rubin, with the result that important vulnerabilities were revealed six months before the code was to be used in the 2002 primary election. But in that case, the posting was accidental, done by a Diebold employee, and not the result of lawbreaking. The fact that good may have come from both the Diebold and Palin incidents does not change the fact that one posting was accidental and the other was a violation of the law.

Most cases that involve privacy risks also involve *security*, and this is no exception. It was shockingly easy for the interloper to break into Palin's account. The interloper gained access by successfully answering "challenge" questions to reset the password on the account. When filling out a request to reset a "forgotten" password, he was asked to enter Palin's birthday and her home zip code, which could be found from Wikipedia and Google, respectively [22]. This led him to the security question, "Where did you meet your spouse?" He searched the Web for this, and soon entered "Wasilla High", and then was allowed to enter a new password, with which he accessed the account.

Obviously, it does not do much good to protect an account with a strong password if the answers needed to reset the password are just a few clicks away. That was the case with Yahoo accounts [23, 24]. A user trying to recover a forgotten password is asked to enter his/her e-mail address. Then (s)he is given the option of e-mailing a new password to an alternate e-mail address, or immediately resetting the password through a form on the current Web page. If the user chooses

an immediate reset, the site prompts with a security question. If the user answers that correctly, the password can be reset.

Security questions offer little protection for accounts of celebrities, for whom a wealth of personal information can be found on the Web [25, 26]. But even ordinary people are vulnerable to an intruder who is moderately skilled at Web searches [25]. A mother's maiden name can often be found through a genealogy search. "What high school did you attend?" can often be answered at Classmates.com.

Yahoo is not the only e-mail services with such an intrusion-prone password-reset protocol. Hotmail and many ISP-provided e-mail services use the same mechanism [27]. Why do they make it so easy to change passwords on their accounts? According to one security vendor [27], it's profit. They do not want users calling help desks to ask for password resets. One call would wipe out a month's worth of profit for the account.

Gmail has a more secure policy [26]. Like the other services, a user can have a new password e-mailed to an alternate e-mail account. And like the others, Google allows a password to be reset with a security question—but only after an account has been inactive for five days. This prevents anyone from breaking into an actively used account by guessing the answer to a security question. Users who forget their passwords are probably not actively using their accounts, so locking them out for five days is a less serious inconvenience.

As a user. what can you do to make it hard for someone to guess the answers to your security questions? One way is to include an arbitrary string of characters in the answer to each security question [28]. Then you know that whenever you answer a security question, you must also enter the arbitrary string. This renders the intruder unable to enter unless he knows the character string as well as the answer to the security question. The article [28] also has good suggestions for creating secure passwords without using the same password on every site.

5. Questions for class discussion

The ramifications of this case can serve as excellent topics for classroom discussion. Let me suggest several questions that a class might be asked to answer.

Why do people use personal e-mail for professional purposes? Perhaps they intend to keep something from their manager's eyes (what information might they be trying to hide?). In almost all cases (excepting whistleblowing, perhaps), this would be unethical. Perhaps they are using the personal account to store large attachments on servers that have more capacity than their work e-mail system. This seems more justifiable, especially if they take care to set the From: address on outgoing mail to match their work e-mail address (this is possible on gmail and perhaps other free mail accounts).

Why do people use professional e-mail for personal purposes? Employers have different policies on personal use of the employer's computer equipment. Some prohibit it entirely, while others (especially universities) allow it if it does not interfere with work-related use of the computer systems. One reason might be so that they see some personal messages (e.g., from their spouse) more quickly. Repeatedly checking a personal e-mail account (or social-

networking site) during the workday might distract them from work-related tasks. If their spouse can phone them during the workday, then shouldn't (s)he be able to e-mail them too? Even if users decide to stop using the same account for personal and professional e-mail, it not be easy to make this change, given that they are in many address books and on many e-mail lists that can't be changed immediately.

Do government employees have different obligations than private-sector employees? As we have seen, government employees are often subject to open-records laws. Similarly, they are frequently prohibited from using the resources of the government to lobby the government, so they might not be able to e-mail their elected officials from their work accounts.

Which are more secure, personal e-mail accounts or professional e-mail accounts? A e-mail account belonging to an employer seems to be more secure, because labor and tax laws require the employer to be able to identify the employee. Thus, it's unlikely that anyone could masquerade as the employee to gain access to the account (but beware of social-engineering attacks!).

Which are more private, personal or professional e-mail accounts? As we have seen, government e-mail is often public record, meaning that anyone can ask to see the contents. That's not true of corporate e-mail, of course, but employees don't have any right of privacy from their employer [29]. Indeed, most companies monitor employee e-mail, and more than a quarter have fired someone for misusing it. By contrast, personal e-mail is private by the Electronic Communications Privacy Act of 1986.

6. Conclusion

The Palin e-mail case is ideal for class discussion because of its timeliness and the fact that it illustrates several dangers regarding use of e-mail. It underlines the distinction between professional and private e-mail accounts, and allows students to see that some activities are off limits on each. It illustrates how precarious our privacy is in the face of search tools that can ferret out personal information on almost all of us. And it accentuates the need for care in choosing passwords and answering challenge questions. It is the author's hope that this case will be used in computer ethics courses to underscore the limits of privacy.

Bibliography

[1] Falcone, M. Charge in Palin e-mail case. *New York Times*, Late edition—final, Oct. 9, 2008

[2] Farhad Manjoo. Gov.Palin@Hacked.com. *Washington Post*, Regional edition, Sept. 21, 2008.

[3] Gohring, N. Over 50% of companies fire workers for e-mail, 'Net abuse. itworld.com, Feb. 28, 2008, http://www.itworld.com/companies-fire-employees-email-080228 [accessed 2/09]

[4] Chai, Carmen, How to use email @ work; Carefully and very professionally, experts suggest, because someone is watching your every move. *Toronto Star*, July 12, 2008.

[5] WRAL-TV. Media: All government e-mails public records. Apr. 3, 2008. http://www.wral.com/news/local/politics/story/2672185/ Accessed in 3/09.

[6] Wright, Benjamin. Local government e-mail and the Freedom of Information Act. http://legal-beagle.typepad.com/wrights_legal_beagle/2008/08/local-government-e-mail-and-the-freedom-of-information-act.html [accessed 2/09]

[7] Weiner, Rachel. Palin's email account hacked. *Huffington Post*, Sept. 17, 2008. http://www.huffingtonpost.com/2008/09/17/palins-email-account-hack_n_127184.html Accessed in 3/09.

[8] Stephey, M. J. Sarah Palin's e-mail hacked. *Time*, Sept. 17, 2008. http://www.time.com/time/politics/article/0,8599,1842097,00.html

[9] Sanchez, Julian. Hack of Palin e-mail makes case for sticking with .gov account, *Ars Technica*, Sept. 17, 2008. http://arstechnica.com/security/news/2008/09/palin-e-mail-hack-makes-case-for-sticking-with-gov-e-mail.ars Accessed in 3/09.

[10] Shear, Michael D. and Vick, Karl. Hackers Access Palin's Personal E-Mail, Post Some Online, *Washington Post*, Suburban edition, September 18, 2008.

[11] McNamara, Paul. Palin's private e-mail hacked, posted to 'Net. Sept. 17, 2008. http://www.networkworld.com/community/node/32838?nlhtspec=rn_091708&nladname=091708 Accessed in 3/09.

[12] British Broadcasting Corporation. Hackers infiltrate Palin's e-mail. Sept. 18, 2008, http://news.bbc.co.uk/2/hi/americas/7622726.stm Accessed in 3/09.

[13] Corn, David. Appeal filed in the case of Sarah Palin's secret emails. *Mother Jones*, Sept. 9, 2008. http://www.motherjones.com/mojo/2008/09/appeal-filed-case-sarah-palins-secret-emails Accessed in 3/09.

[14] Demer, Lisa. Governor's two e-mail accounts questioned. *Anchorage Daily News*, Sept. 15, 2008. http://www.adn.com/sarah-palin/story/526281.html Accessed in 3/09

[15] Jackson, Henry C. Iowa gov starts using state e-mail after scrutiny. *Yahoo Tech*, March 3, 2009. http://tech.yahoo.com/news/ap/20090303/ap_on_hi_te/iowa_governor_e_mails Accessed in 3/09

[16] Sanchez, Julian. Palin comes under fire for using Yahoo e-mail for state biz. *Ars Technica*, Sept. 16, 2008. http://arstechnica.com/tech-policy/news/2008/09/palins-e-mail-habits-come-under-fire.ars Accessed in 3/09.

[17] Sinrod, Eric. Does the indictment of the alleged Palin email hacker hold water? *FindLaw*, 2008. http://technology.findlaw.com/articles/00006/011213.html Accessed in 3/09.

[18] Hunt, S. M. Alleged Sarah Palin hacker facing tougher charges. *TG Daily*, March 10, 2009. http://www.tgdaily.com/content/view/41684/118 Accessed in 3/09.

[19] Hunt., S. M. Palin hacker denies felony charge, and being a "hacker." *TG Daily*, Nov. 14, 2008. http://www.tgdaily.com/content/view/40206/118/ Accessed in 3/09.

[20] Moran, Rich. Palin e-mail hacking brings campaign to a new low. *Pajamasmedia.com*, Sept. 18, 2008. http://pajamasmedia.com/blog/palin-e-mail-hacking-brings-campaign-to-a-new-low/ Accessed in 3/09.

[21] Schwartz, John. A professor's pastime: hacking the voting system; Computer expert is Diebold's worst enemy. *International Herald Tribune*, May 5, 2004, Finance p. 13.

[22] Techweb. Palin E-mail hacker claims Google search helped find password. Sept. 18, 2008. Accessed via Lexis/Nexis Academic in 2/09.

[23] Macronin. Palin's e-mail breached through weak Yahoo password recovery mechanism. *Privacy Digest*, Sept. 20, 2008. http://www.privacydigest.com/2008/09/20/palins+email+breached+through+weak+yahoo+password+recovery+mechanism Accessed in 3/09.

[24] Greg Hughes – dot net. A case study in poor authentication: Palin's Yahoo! email account. http://www.greghughes.net/rant/ACaseStudyInPoorAuthenticationPalinsYahooEmailAccount.aspx Accessed in 3/09.

[25] CyberCrime & Doing Time. Governor Palin's email: security questions in the Facebook age. September 22, 2008. http://garwarner.blogspot.com/2008/09/governor-palins-email-security.html Accessed in 3/09.

[26] Wysopal, Chris. Learning from Sarah Palin's Yahoo mail compromise. September 18, 2008. http://www.veracode.com/blog/2008/09/learning-from-sarah-palin-yahoo-email-compromise/ Accessed in 3/09.

[27] Keizer, Gregg. Tactic used to access VP candidate's e-mail works on the top three services. *Computerworld*, Sept. 19, 2008. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115187 Accessed in 3/09.

[28] Pash, Adam. How to protect your email from hackers. *Lifehacker*, Sept. 18, 2008. http://lifehacker.com/5051905/how-to-protect-your-email-from-hackers Accessed in 3/09.

[29] Guerin, Lisa. Email monitoring: Can your employer read your messages? Nolo. http://www.nolo.com/article.cfm/objectId/C1066E74-A5CA-4EE3-ACD2BE025D8F13CF/catID/81576D30-7E60-45FF-ABDFDFC2B8CB0A8C/104/150/206/ART/ accessed 3/09.