PEEPING

By Peter P. Swire[†]

TABLE OF CONTENTS

---

† Special Assistant to the President for Economic Policy, the National Economic Council; C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University (on leave). The text of this paper was completed before the author entered the United States Government, and the views expressed herein are entirely his own. My thanks to Annie Anton, David Brin, Jonathan Cantor, and Miranda Johnson Haddad for comments from participants at the Berkeley Conference on Security Breach Notification Six Years Later and the Privacy Law Scholars Conference 2009. Special thanks to my research assistants Joseph Buoni, Anthony Frost, Leah Stoecker, and Peter Williams for their good cheer in tracking down sources ranging from Lord Tennyson to technical papers from the Association of Computing Machinery.

Passport peeping—more than just curiosity?[1]

Turns out a lot more people than George Clooney and his girlfriend were hurt by the Hollywood hunk's motorcycle accident last month. As many as 40 doctors and other employees at the Palisades Medical Center in North Bergen, N.J., got suspensions for allegedly leaking confidential medical information about the couple.[2]

Government computers used to find information on Joe the Plumber: Investigators trying to determine whether access was illegal.[3]

I. INTRODUCTION

The 2008 presidential campaign focused unprecedented attention on "employee snooping" into personal files, from the candidates' passports, to Obama's cell phone records, to Joe the Plumber's child support payments.[4] In the same period, a rash of intrusions into celebrities' medical files led to a new California law that imposes monetary sanctions for unauthorized looking into a person's medical files.[5]

This Article explores this phenomenon of employee snooping, a practice I call "peeping."[6] A "peep" may seem a small thing, defined as "to peer slyly or secretly; take a hasty, furtive look."[7] The "peep" is hasty, just taking a moment. It is furtive, suggesting that the person knows that he or she is

---

1. Employees look at passport records of candidates Clinton, McCain, and Obama. Zachary Coile, *Passport Peeping—More Than Just Curiosity?*, S.F. GATE, Mar. 22, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/03/21/MN43VODTF.DTL&type=politics.

2. Leo Standora, *Staff Suspended for Leaking George Clooney Medical Records*, N.Y. DAILY NEWS, Oct. 10, 2007, http://www.nydailynews.com/gossip/2007/10/10/2007-10-10_staff_suspended_for_leaking_george_cloon.html.

3. Randy Ludlow, *Government Computers Used to Find Information on Joe the Plumber: Investigators Trying to Determine Whether Access was Illegal*, COLUMBUS DISPATCH, Oct. 24, 2008, http://www.dispatch.com/live/content/local_news/stories/2008/10/24/joe.html?sid=101 [hereinafter *Government Computers*].

4. *See infra* Part II.

5. *See infra* Section V.B.2.

6. An earlier term for this phenomenon was "browsing." *See* Beverly Woodward, *The Computer-Based Patient Record and Confidentiality*, 333 NEW ENG. J. MED. 1419, 1420 (1995). That term was primarily used, however, before the every-day use of web browsers. Essentially, we all "browse" now, so I think the term "browsing" should not be the label for a category of questionable or even criminal behavior.

7. WEBSTER'S NEW WORLD COLLEGE DICTIONARY (June 2009 revisions).

doing something shameful or blameworthy. "Peep" is further defined as "a look through a narrow aperture . . . into a larger space."[8] In the physical world, that can mean the Peeping Tom who stares out at Lady Godiva. In our computerized world, to "peep" means to look through your computer screen into the large expanses of modern databases.

This Article draws on mythology and literature to show the ancient roots of the phenomenon of peeping. There is a profound ambivalence about how seriously we should treat peeping. The motives to peep are as varied as human nature—to see a handsome or beautiful person, gossip with friends about what you have seen, use the information against your foes, sell the gossip for cash, and perhaps even blackmail someone. As understandable as the impulse is, however, the word "peep" also refers to "furtive" and thus blameworthy activity. As we will see, the penalty to Peeping Tom himself was very severe—a lifetime of blindness.[9] When the foundational story for a phrase imposes such a severe penalty, then we have an important clue that something important is at stake.

Part II of the Article discusses the recent political and celebrity peeping incidents. Part III describes three increasingly harmful types of peeping: the *gaze*, the *gossip*, and the *grab*. Part IV asks: "Why now?" Human curiosity, especially for the titillating or about the famous, is as old as human nature. There are specific reasons, however, why these peeping incidents are coming to our attention now. First, the number of detailed databases, accessible by numerous employees, has climbed sharply in recent years. Second, once a peeping incident occurs, the perpetrator can easily post the evidence to a blog or social networking site. Finally, databases increasingly include logging and auditing software, so that the peepers can be caught after the fact. In short, both the opportunity for peeping and the possibility of catching the peeper have climbed. As a society, therefore, we are newly facing the question of how to respond when we catch the perpetrators.

Part V explores what to do about this increase in peeping. The traditional penalty for peeping was blindness, but that seems a bit excessive. Many of the most promising approaches are technical safeguards, including systems that limit employee access except where authorized and auditing systems to deter, detect, and punish those who break the rules. There are also useful administrative safeguards, from training employees to considering expanding the new California's security breach notification laws to include a notice requirement in the event of a peep.

---

8. OXFORD ENGLISH DICTIONARY (June 2009 revision).
9. *See infra* Section III.A.

Finally, Part VI applies these insights to a major current area of controversy: behavioral advertising on the Internet. A significant source of concern about tracking the Internet usage of individuals is that they will become subject to peeping, as happened for instance to Obama's cell phone records once he became famous. This risk of what Jeffrey Rosen has called "The Unwanted Gaze"[10] gives good reason to assure that effective anti-peeping measures are in place for any behavioral advertising systems that are deployed.

The topic of peeping is fascinating. We all can understand the temptation to peep at something intriguing. We also know that we do not want to be peeped at in our modern hospital, phone, online surfing, or other databases. Perhaps this Article can encourage more discussion about peeping from many fields beyond law and technology, including literature, mythology, sociology, anthropology, psychology, and more.

II. RECENT PEEPING INCIDENTS

Many of the recent stories about peeping arose in the 2008 presidential campaign and in incidents where the medical records of celebrities were compromised. This Article highlights some of the more notable recent incidents before turning to what these incidents mean and what should be done to reduce their effects.

On March 20, 2008 the State Department announced that two employees were fired and a third was disciplined for improperly accessing Senator Barack Obama's passport files.[11] Senior department officials said they learned of the incidents only in response to a reporter's inquiry.[12] Upon investigation, they discovered that contractors for the State Department had improperly accessed the files on at least three occasions.[13] In each instance, the improper access was flagged by a computer-monitoring system that creates special alerts for access to the records of high-profile individuals.[14] The front-line

10. *See generally* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

11. Glenn Kessler, *Two Fired for Viewing Obama Passport File: State Department Investigating Whether Contractors Broke Law*, WASH. POST, Mar. 21, 2008, at A03.

12. *Id.*

13. *Id.*

14. The computer-monitoring system for prominent individuals was created after a 1992 incident in which State Department employees improperly accessed the passport records of then-candidate Bill Clinton, apparently in hopes of finding 1960s-era information that would have been damaging to his presidential campaign. *Passport Breach Being Investigated*, WASH. TIMES, Mar. 21, 2008, http://www.washingtontimes.com/news/2008/mar/21/passport-breach-being-investigated/.

managers, however, apparently did not report the peeping incidents to higher-level managers.

The State Department investigation determined that files of Senators Hilary Clinton and John McCain had also been improperly accessed.[15] In addition to the disciplining of the workers, Secretary of State Condaleeza Rice apologized personally to the three presidential candidates.[16] The incident generated widespread attention, and triggered my own interest in peeping as a research topic. In an interview with the Wall Street Journal, I said, "At least they actually had the systems in place to catch it and they took it seriously."[17] I emphasized that the passport flap, and the firing of employees, could help educate our society about the problem: "It's sending a signal to every data clerk in the country that you shouldn't browse."[18]

Another much-publicized peeping incident occurred after Samuel Wurzelbacher, known as "Joe the Plumber," received repeated mention in the October 15, 2008 presidential debate between John McCain and Barack Obama.[19] Wurzelbacher initially drew public notice when he claimed, in speaking on video with Obama, that Obama would raise his taxes.[20] In the days following the debate, information on Wurzelbacher's driver's license and his sport utility vehicle was retrieved from the Ohio Bureau of Motor Vehicles three times, according to the Columbus Dispatch.[21] The Ohio Department of Job and Family Services admitted that the agency checked whether Wurzelbacher was behind on child support payments, as well as whether he was receiving welfare assistance or owed unemployment compensation taxes.[22] These peeping incidents immediately sparked political controversy within both parties.[23] The Columbus Dispatch reported that "the agency's actions drew outrage throughout the nation."[24]

---

15. Helene Cooper, *Passport Files of 3 Hopefuls are Pried Into*, N.Y. TIMES, Mar. 22, 2008, at A1.

16. *Id.*

17. Amy Schatz, *U.S. News: Congress Raises Call for Data Safeguards*, WALL ST. J., Mar. 31, 2008, at A4.

18. *Id.*

19. *See* Wikipedia, *Joe the Plumber*, http://en.wikipedia.org/wiki/Joe_the_Plumber (last visited June 19, 2009).

20. *Id.*; *see also 'Joe the Plumber' Becomes Focus of Debate* (AP television broadcast Oct. 15, 2008), http://www.youtube.com/watch?v=PUvwKVvp3-o (last visited Aug.1, 2009).

21. Ludlow, *Government Computers*, *supra* note 3.

22. Randy Ludlow, *Checks on 'Joe' more extensive than first acknowledged*, COLUMBUS DISPATCH, Oct. 29, 2008, http://www.dispatch.com/live/content/local_news/stories/2008/10/29/joe30.html.

23. The Ohio spokesman for the McCain campaign said, "It's outrageous to see how quickly Barack Obama's allies would abuse government power in an attempt to smear a pri-

An investigation ensued, which produced no evidence that the Obama campaign had sought Wurzelbacher's records. The multiple accesses to his records, however, led to the resignation of the Director of the Ohio Department of Job and Family Services, the firing of the Deputy Director, and the resignation of an Assistant Director.[25] In addition, Ohio enacted a law in early 2009 creating civil and criminal penalties for improper access of personal information in state databases.[26]

One other notable peeping incident also arose from the 2008 presidential campaign. In late November, CNN reported on an internal company email from a senior Verizon Wireless official revealing that "the personal wireless account of President-elect Barack Obama had been accessed by employees not authorized to do so."[27] Obama spokesman Robert Gibbs said that anyone viewing the records would likely have been able to see phone numbers and the frequency of calls, but that "nobody was monitoring voicemail or anything like that."[28] The Verizon official said that employees who accessed the account for "anything other than legitimate business purposes will face disciplinary action, up to and including termination."[29] Those active in the development of privacy law called for further legal protections; Lee Tien of the Electronic Frontier Foundation remarked that "it's time" to give protection to unauthorized access of phone records "because it really is a violation of privacy to have those kinds of records looked at."[30]

Along with these political peeping incidents, there has been a rash of recent peeping into the medical files of celebrities. In May 2007, the National Enquirer reported that television star Farah Fawcett had suffered a relapse of

---

vate citizen who dared to ask a legitimate question." Ludlow, *Government Computers*, *supra* note 3. The Obama campaign responded, "Invasions of privacy should not be tolerated. If these records were accessed inappropriately, it had nothing to do with our campaign and should be investigated fully." *Id.*

24. *Id.*

25. Posting of Catherine Candisky to Columbus Dispatch, UPDATED: Jones-Kelley Quits, Two Others Departing Over Joe the Plumber Searches, http://blog.dispatch.com/dailybriefing/2008/12/joneskelley_quits_over_joe_the.shtml (Dec. 17, 2008 18:49 EST).

26. H.R. 648, 127th Gen. Assem. (Ohio 2008).

27. *Obama's Cell Phone Records Breached*, CNN, Nov. 20, 2008, http://www.cnn.com/2008/POLITICS/11/20/obama.cell.breach/index.html.

28. *Id.*

29. *Id.*

30. Posting of Jordan Light to 60-Second Science Blog, Obama's Cell Phone Hacked, Privacy Issues Murky, http://www.sciam.com/blog/60-second-science/post.cfm?id=obamas-cell-phone-hacked-privacy-is-2008-11-21 (Nov. 21, 2008 18:05).

cancer, before she had even told her son and closest friends.[31] A UCLA employee was fired for unauthorized access to the files.[32] In October, 2007, actor George Clooney and his girlfriend suffered a motorcycle accident in New Jersey. As many as forty doctors and other employees received suspensions for allegedly leaking Clooney's confidential medical information.[33] Then in March, 2008, UCLA Medical Center took steps to fire at least thirteen workers, and disciplined others, for looking at singer Britney Spears's confidential medical files.[34]

III. THREE KINDS OF PEEPING: THE GAZE, THE GOSSIP, AND THE GRAB

As a typology of peeping, the initial step is "the gaze"—looking where one is not supposed to look, such as Tennyson's Peeping Tom gazing at Lady Godiva or a modern-day Peeping Tom sneaking a peep through a bedroom window. A step worse is "the gossip"—telling others about what one has seen. Either accurate or inaccurate gossip can spread information beyond the original peeper, potentially harming a person's reputation. Even worse is "the grab." It occurs when an employee grabs the personal information for profit, such as through blackmail, often at the behest of an outsider. A recent example is where the National Enquirer paid an employee at the UCLA Medical Center to turn over celebrities' medical records on over thirty occasions.[35]

---

31. Charles Ornstein, *Fawcett's Cancer File Breached: The Incident Occurred Months Before UCLA Hospital Employees Were Caught Snooping in Britney Spears' Files*, L.A. TIMES, Apr. 3, 2008, at 1.

32. *Id.*

33. Leo Standora, *Staff Suspended for Leaking George Clooney's Medical Records*, N.Y. DAILY NEWS, Oct. 10, 2007, http://www.nydailynews.com/gossip/2007/10/10/2007-100_staff_suspended_for_leaking_george_cloon.html.

34. Charles Ornstein, *Hospital to Punish Snooping on Spears: UCLA Moves to Fire at Least 13 for Looking at the Celebrity's Records*, L.A. TIMES, Mar. 15, 2008, at 1.

35. Phillippe Naughton, *Lawanda Jackson pleads guilty to selling celebrity medical records*, TIMES ONLINE, Dec. 2, 1008, http://www.timesonline.co.uk/tol/news/world/us_and_americas/article5272883.ece. For additional details of the Jackson indictment, *see Celebrity Medical Files Indictment*, THE SMOKING GUN, Apr. 29, 2008, http://www.thesmokinggun.com/archive/years/2008/0429082ucla1.html.

A. THE GAZE

The simplest form of peeping is merely to look. Literary scholars, of whom I am not one, call this "the gaze."[36] The presence of the gaze is pervasive in western culture, finding roots in mythology, Judeo-Christian teachings, and English common law.

The stories of Tiresias and Peeping Tom show the mythological and psychological importance of "just looking." In Greek mythology, the young poet Tiresias happens upon the goddess Athena while she is bathing. As told by Alfred, Lord Tennyson:

> And all her golden armor on the grass,
> And from her virgin breast, and virgin eyes
> Remaining fixt on mine, till mine grew dark
> For ever, and I heard a voice that said
> "Henceforth be blind, for thou hast seen too much,
> And speak the truth that no man may believe."[37]

Simply for looking, Tiresias is blinded for life. The stories of Lady Godiva and Peeping Tom are strikingly similar. According to the story, the Lady Godiva pleaded with her husband to cease his crushing taxation on the city of Coventry. He agreed, on the condition that she ride unclothed through the city.[38] The townsfolk agreed to shut their doors to protect the modesty of the Lady during her ride. As told once again by Tennyson, however, a low-born churl named Tom looked when he should not have:

> Then she rode back, clothed on with chastity;
> And one low churl, compact of thankless earth,
> The fatal byword of all years to come,
> Boring a little auger-hole in fear,
> Peep'd—but his eyes, before they had their will,
> Were shrivel'd into darkness in his head.[39]

---

36. Special thanks to literary scholar and friend Miranda Johnson Haddad for her assistance with this section. For an extended and thoughtful analysis of the importance of "the unwanted gaze," see ROSEN, *supra* note 10.

37. ALFRED LORD TENNYSON, THE POETIC AND DRAMATIC WORKS OF ALFRED LORD TENNYSON 489 (2004).

38. Wikipedia, *Lady Godiva*, http://en.wikipedia.org/wiki/Lady_Godiva (last visited June 19, 2009).

39. TENNYSON, *supra* note 37, at 95.

From these stories, even this non-literary law professor can make a few observations. First, what was it about Tennyson and these stories? I leave that for scholars of romantic poetry. Second, we learn the traditional penalty for peeping—a lifetime of blindness. There is a poetic and psychological justice to this punishment, what one might call "an eye for an eye-ing."

The power of "just looking" is echoed in our mythological and religious traditions. In Greek mythology, gazing directly upon Medusa could turn the person to stone.[40] In the Bible, Lot's wife is told not to turn back to gaze at Sodom and Gomorrah. She cannot resist the temptation to look, however, and is turned into a pillar of salt.[41] Gazing is forbidden out of respect for the object. In some cultures, those approaching the king were required to abase themselves, and not gaze directly at the king's face.[42]

Similarly, as explained by Alan Westin in his forthcoming history of privacy in western civilization, the ancient Hebrews created a number of protections against the inappropriate gaze.[43] In the nomadic period, the Hebrews were taught to align their tents so that one family could not see directly into another tent.[44] Later, this requirement of physical privacy was exemplified by the command not to look into a neighbor's courtyard.[45] This meant, in practice, that dwellings were built with special walls, to prevent inadvertent peeping into the dwelling of the neighboring family.[46] Westin writes that this preservation of a private space for the family was part of a cultural regard of privacy that was historically and culturally linked to the individual's rights within the Jewish legal system.[47] Respect was due not only to the king, but also to each individual and family, so rules against inadvertent and disrespectful gazing applied to everyone.

Dislike of the inappropriate and unwelcome gaze extended into western legal culture. As Judge Blackstone commented:

> Eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to

---

40. Wikipedia, *Medusa*, http://en.wikipedia.org/wiki/Medusa (last visited June 19, 2009).

41. *Genesis* 19:26.

42. *See generally* Gary T. Marx, *Forget Big Brother and Big Corporation: What About the Personal Uses of Surveillance Technology as Seen in Cases Such as Tom I. Voire?*, 2 J. LEGAL TECH. RISK MGMT. 24 (2007).

43. ALAN F. WESTIN, PRIVACY IN WESTERN CIVILIZATION: FROM THE HEBREWS AND GREEKS TO THE INTERNET AGE (forthcoming 2010).

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

> frame slanderous and mischievous tales, are a common nuisance, and presentable at the court-leet, or are indictable at the sessions, and punishable by fine and finding sureties for their good behavior.[48]

Such behavior found legal protection: peeping and eavesdropping were punishable under English common law.[49] Peeping and eavesdropping have been punished under a variety of causes of action, including trespass, window peeking, secret peeping, eavesdropping, indecent viewing or photography, violation of privacy, voyeurism, and unlawful photographing.[50] Sometimes prosecutions have occurred under less specific claims, such as disorderly conduct, breach of peace, or prowling.[51] In reviewing the cases, Lance Rothenberg writes, "[C]ourts actively employ the lexicon of privacy rights in the prosecution of these crimes. Therefore, it is clear that criminal law serves as a vehicle for the substantive protection of individual privacy."[52]

B. THE GOSSIP

The next step beyond just looking ("the gaze") is to tell someone what you saw ("the gossip"). In this Article, I resist the law professor's impulse to develop a universal theory of gossip. For our purposes, we first recognize that gossip can cause more types of harm than the gaze. When an individual gazes upon the nude form of Athena or the titillating facts in a celebrity's medical files, he is invading the privacy of the object of the gaze. When the individual tells others, however, additional harms may result to the object of the gaze. The object's reputation may be damaged, with embarrassing results: "Did you know that so-and-so has such-and-such a condition!?" The gossip might spread, leading to loss of employment, denial of insurance, being cast out of a social circle, or other concrete harms.

Even Jewish law recognized the harms of gossip, which in Hebrew is *l'shon hara* or the "evil tongue." The term is synonymous with slander and evil

---

48. DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 2-4 (1978).

49. *Id.* at 4. For other legal discussions of the topic, see generally Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 491-92 (2006); Maria Pope, *Technological Arms Peeping Toms with a New and Dangerous Arsenal: A Compelling Need For States to Adopt New Legislation*, 17 J. MARSHALL J. COMPUTER & INFO L. 1167 (1999); Bill Prewitt, *The Crimination of Peeping Toms and Other Men of Vision*, 5 ARK. L. REV. 388 (1951).

50. Lance E. Rothenberg, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and Failure of the Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1144 (2000) (collecting cases under each heading).

51. *See generally* H. Morley Swingle & Kevin M. Zoeller, *Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Tom*, 52 J. MO. B. 345 (1996).

52. Rothenberg, *supra* note 50, at 1144 (citations omitted).

gossip.[53] Jewish religious leaders equate the harm of gossip, a "heinous crime," to that of murder and idolatry.[54] Rabbis recognized that *l'shon hara* harmed three individual: he who told it, he who heard it, and he who was slandered.[55] One commentator, poignantly remarked, "If [the Rabbis] were horrified by *l'shon hara* in their day, when news took months or years to circulate, consider how they would react today, when words are flashed around the world in an instant."[56]

A political incident from 2008 illustrates the harm of truly awful (great?) gossip. Congressman Vito Fosella from Staten Island was arrested in Northern Virgina for driving under the influence.[57] As it turns out, the Congressman was in there to visit his long-time girlfriend who lived there with their preschool-aged, out-of-wedlock daughter.[58] His girlfriend had to come down to the station house to bail him out because his wife was up in Staten Island with his three acknowledged children.[59] The Vito Fossella story was too good to keep secret. This sort of story could have led to serious professional damage in any era. In our modern era of blogs and 24-hour cable TV, the story spread almost instantly, and the Congressman announced he would not run for re-election.[60]

The negative effects of gossip, however, go far beyond this sort of dramatic story about a public figure.

C. THE GRAB

The most serious form of peeping is the "grab," where an employee accesses records for personal gain, rather than to gaze or gossip. Compared to the gossip, the grab is worse in two respects. First, the law regularly treats an action undertaken for financial gain as more serious. The Health Insurance Portability and Accountability Act[61] (HIPAA) privacy rule, for instance, prohibits the disclosure of medical records, and the Computer Fraud and Abuse

---

53. EDITH SAMUEL, YOUR JEWISH LEXICON 86-87 (1982).

54. *Id.*

55. *Id.*

56. *Id.*

57. Allison Klein, *Fossella Pleads Guilty to DUI in Alexandria*, WASH. POST, Apr. 13, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2009/04/13/AR2009041301007.html; *see also* Tom Jackman, *N.Y. Congressman Convicted of DUI: Whether Jail Required Up to Va. Judge*, WASH. POST, Oct. 18, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101700339.html.

58. *Id.*

59. Klein, *supra* note 57.

60. Jonathan P. Hicks, *Fossella Is Said to Be Ending Re-election Bid*, N.Y. TIMES, May 20, 2008, at B1.

61. 42 U.S.C. § 1320d-6 (2006).

Act[62] punishes unauthorized access to computers. Second, the law also punishes outsiders who bribe or persuade employees to violate a duty owed to their employer. This sort of activity by the outsider is essentially theft from the employer, such as a bribe of a public official[63] or misappropriation of an employer's property.[64]

The two recent instances involving personal information of celebrities exemplify this sort of "grab" of personal information. According to her guilty plea, the National Enquirer paid LaWanda Jackson $4,600 to disclose UCLA Medical Center records on thirty-three occasions in 2006 to 2007.[65] The Enquirer got the medical dirt on celebrities.[66] Jackson got indicted and later pled guilty for a criminal violation of the HIPAA medical privacy rules.[67] The second involves the spectacular wiretapping prosecution against "private investigator to the stars" Anthony Pellicano. Pellicano was convicted in 2008 of carrying out numerous wiretaps in Hollywood, including on behalf of Hollywood stars and executives.[68] Pellicano had a variety of techniques for gaining cooperation from current or former telephone company employees, including acquiring company keys, and having a "ladies' man" develop a group of women employees who would reveal phone records when asked.[69]

This sort of grab of personal records is repugnant. According to the guilty plea, the National Enquirer bribed Ms. Jackson to violate her duty to the hospital and the patients, and Pellicano's clients paid for violations of the wiretap laws. This is similar to the way a blackmailer or other evildoer in a Victorian novel might bribe a servant to steal the personal letters of the master or mistress.

The law not only imposes punishments on the employee who grabs and the outsider who induces the grab. The law may also impose a duty on the employer to take precautions against such grabs. One intriguing discussion of

---

62. 18 U.S.C. § 1030(c)(2)(B) (Supp. 2008).

63. 18 U.S.C. § 201 (2006).

64. United States v. O'Hagan, 521 U.S. 642, 643 (1997) (accepting misappropriation theory of insider trading).

65. Phillippe Naughton, *Lawanda Jackson pleads guilty to selling celebrity medical records*, TIMES ONLINE, Dec. 2, 1008, http://www.timesonline.co.uk/tol/news/world/us_and_americas/article5272883.ece. For additional details of the Jackson indictment, see *Celebrity Medical Files Indictment*, THE SMOKING GUN, April 29, 2008, http://www.thesmokinggun.com/archive/years/2008/0429082ucla1.html.

66. *Id.*

67. *Id.*

68. David M. Halbfinger, *Investigator to the Stars is Convicted in Wiretaps*, N.Y. TIMES, May 16, 2008, at C1.

69. David M. Halbfinger, *In Pellicano Case, Lessons in Wiretapping Skills*, N.Y. TIMES, May 5, 2008, at C6.

this duty appears in a Federal Trade Commission's letter issued after a data breach affected customers of Novastar Financial, Inc. and Novastar Mortgage, Inc.[70] The FTC's investigation considered "whether NovaStar failed to implement reasonable procedures or review its employees' access to consumer reports," in violation of the Fair Credit Reporting Act[71] or the Safeguards Rule of the Gramm-Leach-Bliley Act.[72] The FTC used the letter to highlight the risks created by "rogue employees," and described potentially far-reaching obligations on employers to monitor peeping by employees.[73] It suggested that employers would need to "adjust their information security programs" with the changing tide in technology and risks over time.[74] The FTC suggested that "for companies that allow employees access to highly sensitive data" such measures include,

> depending on the circumstances: tailored access limitations based on an employee's position, functions, and workload; periodic supervisory review of an employee's activity; employee training and clear warnings regarding wrongful access to or disclosure of data; and/or the use of software or other means to monitor employee access to consumer data, place restrictions on such access, or flag suspicious activity.[75]

IV. WHY NOW?

This year's rash of high-visibility peeping cases raises two related questions: has peeping become more common, or is it the *discovery* of peeping that is becoming more common? I offer reasons to believe that both are occurring.

Peeping may have become more common because of a shift in the balance of elements of the classic TV detective questions: did the suspect have the means, motive, and opportunity to commit the crime.[76] While human motives change slowly, the means and opportunity for peeping have risen in recent years. The means of peeping is generally to have access to an intri-

---

70. Letter from Joel Winston, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission to Garrett Rasmussen, Apr. 4, 2008, http://www.ftc.gov/os/closings/staff/080404novastar.pdf [hereinafter Winston Letter].

71. 15 U.S.C. § 1681 (2006).

72. 16 C.F.R. § 314 (2003).

73. Winston Letter, *supra* note 70.

74. *Id.*

75. *Id.*

76. Larry Rogers, *Cybersleuthing: Means, Motive, and Opportunity* (2000), http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2000/summer/security-sum-00.htm.

guing database: the hospital database about the celebrity, the Verizon database about cell phone calls, or the passport database about the presidential candidate. As scholars have frequently noted, the number, size, and granularity of personal-information databases has grown rapidly over time.[77] The opportunity is provided to every employee that can access the database. In the old paper-based world, official records clerks often were involved in each retrieval of a paper file. In the world of mainframe computers, sophisticated technicians assisted in data retrieval. Today, by contrast, the spread of desktops, laptops, and intranets means that numerous employees often have access to the corporate databases. The cliché is that data can be retrieved "at the click of a mouse." Retrieval is not only simple, but can be done furtively from the safety of one's own desk. No nosy file clerk or computer technician stands in the way of peeping into the file.

As technology has increased the mode and opportunity of peeping, so too has it amplified the ability to discover this presumably furtive peeping. The prevalence of electronic files and the ease of dissemination of such files, coupled with the growing presence of data breach laws, have all contributed to the visibility of a once more clandestine act.

The shift from paper to electronic files has increased both the ease of searching for files in a database, and the likelihood of after-the-fact detection of a violation. First, the ease of searching in a database and the lack of the need for physical intrusion into forbidden space makes it easier for an employee to peep on impulse. In the physical world, it takes a significant amount of nerve to walk into a locked room or to open a locked file drawer. On a computer, a person might peep at those George Clooney pictures or Obama records all in an instant. People acting on impulse can easily underestimate the likelihood that their unauthorized access will come to the attention of an audit system at a later date.[78]

---

77. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); SIMSON GARFINKLE, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2001); Jack Lerner & Deirdre Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 15 (2008).

78. Even if they correctly estimate the risk, people who act on impulse, similar in this respect to addicts, may act contrary to their self interest when giving into the impulse. *See generally* Robert Cooter, *Models of Morality in Law and Economics: Self-Control and Self-Improvement for the 'Bad Man' of Holmes*, 78 B.U. L. REV. 903 (1998). A related insight comes from Katherine Strandburg, who describes reasons why people may wish to take privacy-protecting actions but do not achieve their wishes. Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1241-42 (2005).

The shift to electronic files and databases has also allowed for a more easily traceable electronic footprint. In the past, when an employee goes into a locked room or a locked file drawer to look at forbidden files, the chance of detection after an incident of peeping was usually slight. By contrast, few employees know all the intricacies of the logging and audit software in a modern computer system. In many systems, the audit logs might be reviewed much later, perhaps after suspicion of an incident. Once the investigation begins, a peep can potentially be detected, even months or years later.

Furthermore, peeping gets discovered more often now because of the ease of disseminating information. In the paper-based world, the peeper would often keep the knowledge close, perhaps gossiping with a few friends. In the world of blogs and the Drudge Report, the barriers to propagation are much lower. Juicy gossip by its nature is often repeated. When the gossip is in a blog or an often-forwarded email,[79] the details in the original revelation can be readily spread to a mass audience. Once the peeping is widely known, as with the examples cited at the beginning of this Article, there is greater pressure to "do something" to punish the violator.

With this greater pressure to act, the shift from paper files to electronic, audited systems also affects the way that peepers are detected and punished. In a paper-based world, the perpetrator is caught locally, such as by a co-worker who happens to spot a violation. The punishment is likely to be local as well—the sort of shaming or administrative sanction that occurs for other local and non-criminal violations. By contrast, a peeper into the electronic database may be discovered by an auditing specialist or in the course of an actual investigation. The informal sanctions within the work community can then give way to more formal sanctions within the hierarchy.

Finally, the growing prevalence of data breach laws and reports of peeping in the press have likely increased the official attention paid to peeping incidents in an organization. Managers and IT administrators now run a greater risk of criticism if they become aware of a peeping violation but do nothing about it.

---

79. My own perspective on often-forwarded emails is formed in part by the widely circulated email exchange from 2000 of Ms. Claire Swire (no relation) and her male friend, Bradley Chait. The story of the off-color email is told at Snopes.com. *Under the Yum-Yum Tree*, SNOPES, http://www.snopes.com/risque/tattled/swire.asp (last visited June 19, 2009). On the day of this writing, the charming email comes up next to my own home page on a Google search for "Swire."

V. WHAT TO DO ABOUT PEEPING?

This Article on peeping seeks to focus our attention at the issue—to gaze at it—rather than to perform a comprehensive cost/benefit analysis of the possible response. The discussion above indicates that peeping is likely more common in our database-filled world and that it is likely to be detected more often, especially because of the audit and logging features of modern computer systems.

At least two contradictory impulses affect our opinion of peeping. The first is whether the "harm" is a serious one. One strand of privacy law in recent years has focused on the concrete, and often financial, "harms" caused by privacy invasions. Enforcement efforts have focused on topics such as identity theft, where an individual can have a bank account hijacked or suffer other monetary loss. Other regulatory efforts have focused on sensitive medical and financial information, where improper leaks of medical data might lead to loss of insurance, or improper data in a credit history could lead to mistaken denial of a mortgage or other loan. By contrast, there is usually no similar financial harm from simple peeping, whether it is an employee looking at the Obama passport photo, Joe the Plumber's motor vehicle records, or an ordinary individual's records. On the view that "harm" means concrete economic harm, peeping appears like a trivial matter, unworthy of legal or policy attention.

The contradiction arises when the press reports, for Joe the Plumber's records, that "[t]he agency's actions drew outrage from across the nation."[80] The stories of Tiresias and Lady Godiva suggest a deep historical and psychological concern about peeping—something important is going on here.

A parallel contradiction arises in terms of the appropriate punishment for peeping. Along with the ancient stories that impose harsh punishments for peeping, there exists federal precedent for treating peeping quite seriously. Unauthorized inspection of federal tax returns, for instance, can lead to imprisonment for up to a year, and federal employees are stripped of civil service protections and mandatorily dismissed from office upon conviction.[81] In addition, federal agency codes of conduct under the Privacy Act provide that records may only be disclosed to employees who have a legitimate need to access the records in the course of official duties.[82] On the other hand, any employee who quickly peeped at George Clooney's x-rays would believe that

80. *See supra* note 24.

81. 26 U.S.C. § 7213A (2006).

82. *E.g.*, Social Security Administration Employee Standards of Conduct, 20 C.F.R. § 401, App. A, (54d)(1)(c) (2007).

blindness, or even a year in jail, is an excessive punishment. The employee would argue that the peeping was at most a social misdemeanor, something one should not do perhaps, such as gossiping a bit too much or too nastily, but not an offense that would warrant such severe sanctions.

In facing these contradictory impulses, the prudent course is to find ways to prevent the temptation to peep and reduce its prevalence. A basic principle of privacy law is that there should be "appropriate administrative, technical, and physical safeguards." Such language appears, for instance, in the Privacy Act of 1974[83] and in the HIPAA medical privacy rule.[84] Many of the most promising responses to the risk of peeping are either technical or administrative safeguards. Though physical safeguards, such as preventing a stranger from seeing a celebrity's medical records, they are appropriate going forward, they are less likely to be the crucial measures for preventing peeping into databases.

A. TECHNICAL SAFEGUARDS

Many of the best responses to peeping are technical safeguards. Although a complete security system includes numerous safeguards, the discussion here will briefly examine four of them: role-based access control, special treatment for famous or very important persons (VIPs), masking and de-identification techniques, and audit logs. Each of these measures is used by state-of-the-art systems today. These measures are more commonly deployed in the health care sector, which is regulated and has a long history of confidentiality. However, the risk of peeping suggests that these safeguards should be deployed more widely and consistently.

1. Role based access controls.

Role based access control (RBAC), also called role-based security, is a computer security technique for assuring that only people in authorized "roles" can do particular activities in a computer system.[85] Effective deployment of RBAC, for instance, could limit who could access the files of a celebrity or other individual. The academic understanding of RBAC has devel-

---

83. 5 U.S.C. § 552a(e)(10) (2006). The statute says that the safeguards are to protect "against any anticipated threats or hazards" that "could result in substantial harm, *embarrassment*, inconvenience, or unfairness to any individual on whom information is maintained." *Id.* (emphasis added) The inclusion of "embarrassment" on the list shows recognition of a sort of harm that can happen to a person from peeping, even if there is no tangible financial loss.

84. 45 C.F.R. § 164.530(c) (2006).

85. National Institute of Science and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control (RBAC) and Role Based Security, http://csrc.nist.gov/groups/SNS/rbac/ (last visited June 19, 2009).

oped considerably in the past fifteen years.[86] The American National Standards Institute adopted an industry consensus standard for RBAC in 2004,[87] and most information technology vendors have now incorporated RBAC into their product lines.[88]

The increased use of RBAC, perhaps combined with purpose-based access controls,[89] would reduce the range of employees in an organization who could peep into an individual's files. For instance, persons treating a patient or doing customer service for an individual would have access to files, but other employees would not. The HIPAA privacy rule contained a requirement that only the "minimum necessary" personal health information be used or disclosed by a hospital or other covered entity.[90] The rule announced the principle of role-based access:

> A covered entity must identify: (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.[91]

Currently, RBAC is likely deployed most commonly in sophisticated computer systems and those that are regulated by HIPAA to use or disclose only the minimum necessary information. RBAC is less widely used in smaller and less sophisticated systems, including for smaller medical practices.[92]

---

86. National Institute of Science and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control—Frequently Asked Questions, http://csrc.nist.gov/groups/SNS/rbac/faq.html (last visited June 19, 2007).

87. INCITIS, AMERICAN NATIONAL STANDARD FOR INFORMATION TECHNOLOGY—ROLE BASED ACCESS CONTROL 359 (2004), *available at* http://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf.

88. National Institute of Science and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control (RBAC) and Role Based Security, http://csrc.nist.gov/groups/SNS/rbac/ (last visited June 19, 2009).

89. Computer scientist Annie Anton commented that role-based access (e.g., doctor, IT manager) should be enhanced with purpose-based access (treatment, system security), which may be more granular and less subject to a highly privileged role getting access to too many records. For a discussion of purpose-based access, see Naikuo Yang et al., *A Purpose-Based Access Control Model*, 1 J. INFO. ASSURANCE & SEC. 51 (2008).

90. 45 C.F.R. § 164.514(d)(2) (2006).

91. *Id.* The requirement to comply with these minimum necessary standards, however, does not mean that all health care providers have implemented the formal, complete systems that researchers would consider fully RBAC systems.

92. The HIPAA privacy rule is "scalable," meaning that entities may take into account the cost burden of implementation, consistent with the entity's size and sophistication, when

However, a significant limitation of RBAC remains. Peeping can occur by all those whose "roles" allow them access to the full file. For instance, a number of the medical peeping incidents involved doctors and nurses whose role provided them access to the files (but who were not supposed to be looking at non-patients such as the celebrities at issue).[93]

Regardless, RBAC is a promising path for reducing the range of employees who can peep into files. In short, RBAC should be more widely deployed in the future, and will provide a significant but incomplete protection against peeping.[94]

2. VIP Treatment

The experiences of Senator Obama and movie stars such as George Clooney are recent evidence that VIPs are especially likely to be the subject of peeping. One logical response is to provide additional safeguards for these VIP files.

Based on my experience with medical providers and others, this sort of VIP treatment was often done in paper-based records. In a paper-based world, the safeguards are relatively easy to create: a supervisor and perhaps a small set of trusted persons have keys to the special file cabinet. In that way, file clerks and other employees cannot gain access to the VIP files except with the permission of the supervisor.

Creating a VIP system is more complex in a modern computerized system, such as a health system where a wide range of persons often has access to a patient record for purposes of treatment, payment, and health care oper-

---

deciding how to comply with certain provisions. 45 C.F.R. § 164.306(b) (2006). In addition, HHS has provided considerable flexibility about how to implement the role-based requirements: "[T]he Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard." U.S. Dept. of Health & Human Services, Health Information Privacy, HIPAA, Frequently Asked Questions, http://www.hhs.gov/ocr/privacy/hipaa/faq/limited/208.html (Last visited Oct. 7, 2009).

> [The] covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity may develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

Id.

93. *See supra* Part II (discussing recent medical peeping incidents).

94. For a recent account of RBAC, which is generally consistent with the approach in this essay, see Brian Cleary Aveksa, *Peeping on Celebrity Files—How to Gain Control*, ZDNET, Feb. 24, 2009, http://news.zdnet.com/2100-9595_22-272326.html.

ations.[95] Because such a wide range of employees has reason to access a medical record, and employees expect instant access to do their jobs, it can become a daunting technical challenge to enable effective care, billing, and other services for the VIP while not exposing the VIP's records to a large number of employees.

Despite these technical challenges, major health care organizations have recognized the importance of creating special handling procedures for VIPs. The American Health Information Management Association, for instance, states: "Special circumstances may arise in which patient identification or access to individual patient records may require anonymity or special precautions, such as in the case of celebrity or high-profile individuals, workplace privacy, domestic violence, child or vulnerable adult abuse, litigation, organ donors, and prisoners."[96] Similarly, the importance of VIP treatment is built into the coding system for health care records developed by Health Level 7 (HL7), a major health standards body.[97] HL7 has developed a structured code set to govern access to confidential medical records. The code set includes a "C" for "celebrity," and states: "Celebrities are people of public interest (VIP) including employees, whose information require special protection."[98]

In many respects, creating special rules for access to VIP files is an example of role-based access—the rules are stricter about which "roles" are able to access those records. VIP procedures can employ a variety of techniques. For instance, the VIP might use an alias, her records might not be visible in the system unless a code is provided, the record might say that a supervisor's permission is needed for access, or there could be a warning that access is audited and unauthorized access will lead to penalties. VIP files might also be subject to more intensive auditing, as discussed further below.

Looking ahead, the increased incidence of peeping suggests there should be renewed attention by software designers and system administrators to the

---

95. For analysis of the wide range of uses of a modern health record in the United States, see Charles Safran et al., *Toward a National Framework for the Secondary Use of Medical Information*, AMERICAN MEDICAL INFORMATION ASSOCIATION, Sept. 2006, *available at* http://www2.amia.org/inside/initiatives/healthdata/2006/finalpapertowardanationalframeworkforthesecondaryuseofhealthdata_09_08_06_.pdf.

96. Linda Barbera et al., *Ensuring Security of High-Risk Information in EHRs,* 9 J. AHIMA 79 (2008), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039956.hcsp?dDocName=bok1_039956.

97. "Health Level 7 is one of several American National Standards Institute (ANSI)-accredited Standards Developing Organizations (SDOs) operating in the healthcare arena." Health Level 7, *What is HL7?*, http://www.hl7.org/ (last visited June 10, 2009).

98. Health Level 7, *High-Level Overview of the Health Level Seven (HL7): Consent related vocabulary including Confidentiality Codes*, http://www.oasis-open.org/committees/download.php/30930/hl7confidentialitycodes.doc (last visited June 10, 2009).

usefulness of VIP sub-systems within larger computer systems.[99] Creating manageable VIP systems may deserve greater attention in information sharing systems, such as proposed new national systems for electronic medical records. It may seem un-egalitarian and perhaps even un-American to give "special" treatment to the records of some individuals. The experience of Joe the Plumber, who suddenly became famous and then was subject to peeping in the same week, shows the need for good systems that apply to all persons. Nonetheless, the recent peeping incidents have largely involved persons who were already famous, and we should update our ways to handle those records securely.

3. Masking and de-identification

A promising way to stop peeping is to use technical measures that mask the identity of the individual or perhaps entirely de-identify the records. Masking techniques such as encryption and one-way hashes should be strongly encouraged for many security reasons, as well as to reduce the incidence of peeping.

To take a well-known example, data can be encrypted on a hard drive or when being sent to another person. If the hard drive is lost, or a hacker intercepts the communication, the encryption can make it difficult or impossible for the outsider to read the data. This sort of encryption can be effective as well at preventing employees from peeping at data. For instance, if an employee gains access to a hard drive or computer file, but does not have the encryption key, then the employee cannot peep at the data.

Another important category of masking techniques is called the "one-way hash."[100] Essentially, this technique employs mathematical functions that are simple to compute in one direction but very hard to compute in the opposite direction. Applied to personal information, a one-way hash would convert "Peter Swire" to something like "X145-GHWR-T89G." The same one-way hash could be computed each time that "Peter Swire" was run through the mathematical calculator, but it would be very difficult to figure out the name "Peter Swire" if you only have the "hash" of that name.

---

99. One response by the State Department to the passport peeping incidents was to increase the number of persons on the list of people subject to VIP procedures. United States Department of State and the Broadcasting Board of Governors, Office of Inspector General, *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*, AUD/IP-08-29, 39-42 *available at* http://oig.state.gov/documents/organization/109112.pdf (last visited June 10, 2009).

100. For a concise explanation of one-way, or cryptographic, hashes, see Wikipedia, *Cryptographic Hash Function*, http://en.wikipedia.org/wiki/One-way_hash (last visited June 10, 2009).

These one-way hashes can be useful in a wide range of settings where a person's data is shared but only with the person's identity masked by the one-way hash. If the information sharing is structured properly, then the sharing can allow linkage of records of the same person's records, and most or all of the people involved will not know the actual identity of the person. For medical records and other records that today are shared in multiple systems, greater use of one-way hashing will permit the data usage to go forward while masking the identity of the individuals. In short, there can be a range of data uses, while avoiding the risk of peeping.[101]

I recently drafted comments on this topic with the Markle Foundation, the Center for Democracy and Technology, and others.[102] U.S. Department of Health and Human Services (HHS) has proposed the first national guidelines for data breaches involving personal health information. The proposed guidelines include an exclusion for entities employing strong encryption: where effective encryption is in place, covered entities will not need to send notices in the event of a data breach. However, our recently drafted comments emphasize that such notice exclusions should be available only to databases and data formats resistant to unauthorized access.[103] These limited exclusions should incentivize entities who store personal health care data to use state of the art protections and technologies.[104] By encouraging use of effective encryption and one-way hashing, there will be stronger technical barriers in place to prevent peeping.

While we should encourage the use of masking technologies, they are certainly no panacea. Modern computer security researchers, including La-Tanya Sweeney,[105] have shown serious challenges to successful masking of data. This research provides strong reason to consider administrative safeguards, such as nondisclosure contracts, in addition to technical measures for de-identifying data.[106] The basic insight from the researchers is simple and

---

101. For applications to the health care sector, see PETER P. SWIRE, RESEARCH REPORT: APPLICATION OF IBM ANONYMOUS RESOLUTION TO THE HEALTH CARE SECTOR (2006), *available at* http://www.peterswire.net/anon.resolution.whitepaper.pdf.

102. Peter P. Swire, *CAP Comments on HHS Health Data Breach Guidelines*, CENTER FOR AMERICAN PROGRESS, May 22, 2009, *available at* http://www.americanprogress.org/issues/2009/05/data_breach_comments.html. The filed comments are available at http://www.americanprogress.org/issues/2009/05/pdf/MarkleCDTCAPGuidanceComments.pdf.

103. *Id.*

104. *Id.*

105. Dr. Latanya Sweeney's Home Page, http://privacy.cs.cmu.edu/people/sweeney/ (updated Fall 2007).

106. I have participated in a process with the Health Privacy Project of the Center for Democracy and Technology to make recommendations on how to update the de-identification provisions of the HIPAA privacy rule. One theme emerging from this process

profound. In a world of effective search engines, a researcher can often narrow down the identity of people using information available on the Web, and those searches become even more likely to be effective in a world of social networking, where individuals regularly reveal their date of birth and other revealing information.[107]

Although techniques exist to unmask data in some circumstances, peeping will be less common if masking techniques are widely adopted. The above discussion of "the gaze" and "the gossip" showed that peeping can arise from a spur-of-the-moment impulse to see something intriguing or tell others about the tidbit. This sort of peeping is far less likely to occur if the cost of peeping includes tricky encryption research to unmask the hidden identity of individuals. As stated in the recent comments, the use of masking techniques such as encryption and one-way hashing will result generally in better data protection than their absence. The possibility of attacks by determined experts should not detract from the usefulness of protections that prevent accidental or casual data losses.

4. Logging and audits

Effective auditing is a crucial safeguard against peeping. Computerized systems can readily log actions by employees and audit those logs after the fact. Auditing provides the ability to deter, detect, and prove violations of a security policy.[108] The ability to perform audits serves as a deterrent because system users would know in advance that logging and auditing are being used to identify policy violations, such as peeping. The perception that a system is effectively logged and will be audited can thus reduce violations by users.

---

is the important of supplementing technical measures with data use agreements and other administrative safeguards. *See* Posting of Lygeia Ricciardi to PolicyBeta Blog, Health Data De-Identification Rules in Need of Update?, http://blog.cdt.org/2008/11/13/health-data-de-identification-rules-in-need-of-update/ (Nov. 13, 2008).

107. Date of birth is especially individuating because it splits the population into over 25,000 categories (366 days of birth times 80 years equals 28,880 categories). By contrast, a data field for gender splits the population into two categories in most systems; so labeling someone "male" or "female" is far less likely to identify an individual uniquely than providing date of birth.

108. The discussion here closely follows an auditing paper for which technologist Jeff Jonas and I were lead authors. Markle Foundation, Markle Task Force on National Security in the Information Age, *Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability*, 6 (2006), *available at* http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf. For auditing in the context of sharing of electronic health records, see *Auditing Access to and Use of a Health Information Exchange*, *in* THE CONNECTING FOR HEALTH COMMON FRAMEWORK (Markle Foundation, 2006), *available at* connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf.

Detection occurs when an actual policy violation is uncovered after the fact. Detection can occur as a result of sampling, when one of the transactions selected for random audit reveals a violation. Detection can also occur in the context of a specific investigation, when the actions of a suspect are examined carefully and a violation is detected. If there is a credible record-keeping system in place, audits can be used to create evidence of a violation.

The ability of logging and auditing to deter, detect, and prove policy violations is enhanced for computer-based as compared to paper-based systems. It is true that paper-based systems create logs of activities: "sign here to take out this file or library book." In practice, however, logs of computer activity are generally more automatic and comprehensive. For instance, modern software systems routinely audit each access to a corporate database, generate reports for managers of anomalous activity, and provide detailed logs in the event of an investigation.[109] The amendments to HIPAA in the American Recovery and Reinvestment Act of 2009, for instance, require greatly increased accounting of access to files for all computerized systems as of January 1, 2014.[110] Few paper-based systems in practice match this level of detailed logging and auditing.

As discussed above, the existence of computerized logging and auditing is a major reason to expect greater detection of peeping in the future. With the increased investment over time in computer security,[111] detailed logging and auditing are becoming increasingly standard features of a wider range of computerized activities.

This increased deployment of logging and auditing is a good trend for computer security in general and addressing peeping in particular. Auditing can raise issues of employee privacy, and best practices should be deployed so that the auditors themselves do not peep.[112] To address peeping, however, perhaps the best single policy to use with audits is to announce to employees that the logging and auditing are occurring. For instance, users of a hospital computer system might see a warning once a week or once a month such as this: "Your access to patient medical records is audited. Accessing patient

109. I gained experience with database audit systems when I served on the Advisory Board to Sentrigo, Inc., a software company that provides database security solutions. SENTRIGO, www.sentrigo.com (last visited June 10, 2009).

110. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

111. On the relatively recent rise of cybersecurity as a policy concern, see Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1975, 1977-78 (2005).

112. My previous work on audits has addressed this concern in various ways, including proposals for how to audit the auditors. Markle Foundation, *supra* note 108.

records outside of those needed for your work will be detected and can lead to serious consequences, including termination of employment. For further information, see our organization's auditing policy." This sort of warning, along with appropriate training, can improve the deterrence effect of auditing on peeping.[113]

B. ADMINISTRATIVE SAFEGUARDS.

Administrative safeguards complement the available technical measures. These administrative safeguards include: training and employment sanctions; a data breach requirement for peeping; and possibly other measures that help teach employees that peeping is not appropriate.

1. Training and Employment Sanctions

One obvious measure to address peeping is to train employees not to do it. The recent high-profile cases can send this message to employees in stark terms: the State Department fired contractors who looked at the passport files, UCLA fired people who looked at Britney Spears' files, over forty employees were suspended for looking at George Clooney's medical files, and a senior official in Ohio resigned in the wake of peeping into Joe the Plumber's files. This sort of training is exceptionally easy: show intriguing pictures of Britney Spears and George Clooney to get everyone's attention, followed by a simple slide: "FIRED".

I suggest that the recent peeping cases are analogous to the Anita Hill case. The language we use about peeping is similar to the way sexual harassment was often described prior to the 1991 confirmation hearings for Justice Clarence Thomas, where Anita Hill presented evidence of sexual harassment when she worked for Thomas.[114] The description goes roughly like this: "It may be a bit improper, but it is a normal part of the workplace. People are just like that, and give in to the understandable temptation to do it. It is not worth making a big legal fuss over, though, and people certainly shouldn't be fired or pay large damages due to it." Read that quote as it applied to sexual harassment before 1991, and as it applies to peeping today.

I am not saying that peeping at a person's files is the same as sexually harassing that person. Instead, I am pointing out there are episodes when our society comes to realize that behavior is occurring that deserves to be treated more seriously than previously. The Clarence Thomas hearing was such a

113. If an auditing program is announced to employees, but employees learn over time that no enforcement occurs, then the deterrence effect would obviously be reduced.

114. *See* Susan K. Hippensteele, *Mediation Ideology: Navigating Space from Myth to Reality in Sexual Harassment Dispute Resolution*, 15 AM. U. J. GENDER SOC. POL'Y & L. 43, 44-45 (2006).

moment for sexual harassment, and the recent passport and other episodes may constitute such a moment for peeping. There are various reasons for believing peeping is a significant issue worth addressing—the concluding discussion in this paper, about online behavioral advertising, suggests that controlling peeping is a key part of controlling the enormous new data collections that occur with modern computer technology.

In terms of policy recommendations, training about peeping can become a more regular part of the training that many organizations already provide about computer security, including complying with medical, financial, and other specialized privacy and security laws. Training should be especially prominent for employees who have regular access to many celebrity and other sensitive records. Institutions should consider writing formal policies about peeping, as they have done for sexual harassment and other compliance issues. And suspension, firing, and other job actions should continue to be imposed, as they have been in recent peeping cases.

2. Data breach notices for peeping

Since California enacted the first data breach statute in 2003, the vast majority of states have passed laws requiring notice to individuals when unauthorized persons breach security and gain access to Social Security Numbers, financial account numbers, and other sensitive information.[115] The rising incidence of peeping poses the question of whether such statutes should extend to peeping.

There is at least one significant distinction, however, between the traditional data breach notice and a peeping notice. One rationale for the data breach notice is that it alerts the individual to possible identity theft, such as where the Social Security Number or credit card number has been compromised.[116] The notice can thus prompt individuals to monitor their credit history more closely or take other protective measures. By contrast, it is unclear what an individual should do upon receipt of a peeping notice.

That question returns us to the issue of appropriate punishment for peeping. California once again broke new ground by passing what I believe is the first statute requiring notices for peeping. Governor Schwarzenegger signed Senate Bill 541 and Assembly Bill 211 on September 30, 2008, and the

115. *See* Milton Sutton, *Security Breach Notifications: State Laws, Federal Proposals, and Recommendations*, 2 ISJLP 927 (2006) (collecting and analyzing state data breach laws). Perhaps the Governor's own celebrity status made him more inclined to support a law that responded to peeping into celebrities' medical files.

116. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 955-58 (2007).

laws took effect on January 1, 2009.[117] The new laws are somewhat complex.[118] For our purposes, the key definition is what counts as "unauthorized access." It is "the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use."[119] For this peeping, this "unauthorized access," a report must be sent to the affected patient or patient's representative and to the California Department of Public Health (CDPH) no later than five calendar days after violation has been detected by the facility.[120] CDPH may assess an administrative penalty of up to $25,000 per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed, and fines of $100 per day can begin after the five days.[121]

The new California laws impose administrative fines on the organization, and the organization quite possibly will suspend, fire, or impose other employment penalties on the person who peeps. In my view, the California approach to penalties is a plausible one.[122] Appropriate responses by the organ-

---

117. S.B. 541, 2007–2008 Reg. Sess. (Cal. 2008); A.B. 211, 2007–2008 Reg. Sess. (Cal. 2008).

118. For two law firm analyses of the new bills, see Shirley P. Morrigan & M. Leeann Habte, *California AB 211, SB 541 with Guest Foley & Lardner*, Feb. 25, 2009, http://www.fairwarningaudit.com/documents/2009-0225-AB211-SB541-FW-FOLEY-FULL.pdf; Kevin D. Lyles & Colin Leary, *California Expands Medical Privacy Laws with New Standards, Oversight, and Administrative Penalties*, JONES DAY, Dec. 2008, http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S5675.

119. CAL. HEALTH & SAFETY CODE § 130201(e) (2008).

120. CAL. HEALTH & SAFETY CODE § 1280.15(b)(1)-(2) (2008).

121. CAL. HEALTH & SAFETY CODE § 1280.15(a), (c) (2008).

122. CAL. HEALTH & SAFETY CODE § 1280.15 (2008). As one additional administrative measure, we can consider a suggestion raised in conversation with me by David Brin, the science fiction writer who wrote The Transparent Society. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998). One of Brin's major themes is reciprocity. For instance, he suggests that the remedy for too many police video cameras is for the public to be able to watch video feeds of the police offices as well. For peeping, Brin asked me to imagine that the peeper's own records would be turned over to the person who was the subject of peeping. For instance, a file clerk who peeped at George Clooney's records would have her own records sent to him. I don't think I support this as an actual public policy matter. But I find it an intriguing thought experiment. Brin is essentially enforcing the Golden Rule, where you should do unto others as you would have them do unto you. Brin is using an age-old device of the parent to the misbehaving child: "Don't look at that person's photos and file. How would you like it if the kids at school were looking at those awful pictures of you from when you were sick last year?" Brin's suggestion shows the element of personal moral choice that the person faces when he or she is tempted to peep. This essay suggests a number of technical and administrative safeguards to reduce the problem of peeping. A related "safeguard" is to raise awareness about why peeping is not appropriate, and to find a fuller set of ways to communicate that it is wrong to peep. Otherwise, in our world of pervasive databases, the incidence of peeping may become unnecessarily great. The Anita Hill incident exemplifies how a con-

ization can reduce the fine, and small organizations are not held to as strict a standard for their systems as large organizations. In short, the approach is to have significant enough financial penalties to induce compliance, but to limit the size of the penalties so they do not spiral out of control.

An intriguing question is whether California's new peeping bill will spread across the country the way that its data breach bill did. One advantage of the peeping bill is that it sends a clear message of public morality—employees are not supposed to peep at patients' medical records.[123] A related argument for the peeping notice bill is that the notices will prompt organizations to take peeping more seriously, helping ensure that technical and other safeguards are put in place.[124] From my own experience working with organizations on data breaches, a breach and the accompanying notices prompt management and employees to examine their practices and often to change them. For instance, it might be easier for an organization to justify investing in masking and auditing technologies once it has gone through the experience of sending notices about a data breach or peeping incident. This improvement in data practices may well justify adopting the California peeping notice approach to a wider range of circumstances.

VI. PEEPING , PRIVACY "HARMS," AND BEHAVIORAL ADVERTISING

This Article has tried to begin a conversation about the topic of peeping. The Article has discussed our deep ambivalence about the phenomenon—it is a serious violation to peep at the records of candidate Obama, Joe the Plumber, or a movie star, but then again it is an understandable human foible that leads us to peep and then gossip about it.

---

sciousness-raising incident can educate a broader public that a practice, such as sexual harassment, is illegal. On consciousness-raising, see Judith Resnick, *Gender, Race, and the Polictics of Supreme Court Appointments: The import of the Anita Hill/Clarence Thomas Hearings: Hearing Women*, 65 S. CALIF. L. REV. 1333, 1333-35 (1992); Noelle Brennan, *Hostile Environment Sexual Harassment: The Hostile Environment of a Courtroom*, 44 DEPAUL L. REV. 545, 545 (1995).

123. On the ability of law to express norms and moral values, see Richard H. McAdams, *The Legal Construction of Norms: A Focal Point Theory of Expressive Law*, 86 VA. L. REV. 1649, 1717-19 (2000); Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 397-400 (1997).

124. For evidence that data breach notice laws have led to greater funding for computer security and stricter data practices, see CHRIS JAY HOOFNAGLE & JENNIFER KING, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 20-21 (Samuelson Law, Tech. & Pub. Pol'y Clinic 2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf.

Upon reflection, I have come to the view that we do sympathize with the employee who gives in to temptation and peeps at the intriguing file. But we also want the *system* to protect us from being the target of peeping.

This insight—the importance of the system protecting us from peeping—bears directly on important current privacy debates and the definition of what counts as a privacy "harm." A major current debate concerns behavioral advertising online.[125] The FTC states that "[o]nline behavioral advertising involves the tracking of consumers' online activities in order to deliver tailored advertising."[126] Proponents of behavioral advertising cite various benefits. Individuals can benefit from personalization, such as by having content or advertisements that better fit the individual's interests.[127] Companies can benefit from targeted advertisements, getting their messages out to the most relevant consumers.[128] Even more broadly, an emerging argument is that behavioral advertising is essential to pay for "free" content online—this type of advertising is the last, best hope for the newspaper industry to pay for investigative journalism and the other expenses of an independent news media.[129]

Defenders of privacy have offered various explanations about what is worrisome about behavioral advertising. One line of argument, advanced by Jeff Chester and others, is that behavioral advertising is bad due to the manipulation inherent in other types of advertisement, only more so.[130] A First Amendment argument, to counter the idea that advertising helps newspapers,

---

125. *See* F.T.C. STAFF, SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 47-48 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf; Peter P. Swire & Annie I. Antón, *In Regards to the FTC Staff Statement, 'Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles,'* April 10, 2008, *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080410swireandanton.pdf; *see also* PeterSwire.net, Behavioral Advertising, http://www.peterswire.net/psbehavioraladvertising.htm (last visited June 20, 2009) (papers from seminar on Behavioral Advertising).

126. F.T.C. STAFF, SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 8, (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

127. *Id.*

128. *Id.* at 3.

129. Thomas M. Lenard & Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, TECH. POL'Y INST. 23 (2009), *available at* http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf. For a somewhat similar approach, see J. Howard Beales III, Public Goods, Private Information, and Anonymous Transactions: Providing a Safe and Interesting Internet (May 7, 2009) (on file with author).

130. Posting of Jeff Chester to Digital Destiny, Tracking You Offline for Better Targeting You Online: Why the FTC and Congress Need to Protect Consumers, http://www.democraticmedia.org/jcblog/?p=817 (May 26, 2009); *see generally* Postings of Jeff Chester to Digital Destiny, http://www.democraticmedia.org/jcblog/.

is what Julie Cohen has called the "right to read anonymously."[131] Under this argument, and as recognized historically by special privacy laws for cable television and newspapers,[132] it is risky to have the content of what we read or see be subject to surveillance. Next, there are concerns that the government might seize the browsing data for national security, law enforcement, or other surveillance purposes. The most widely made privacy argument to date, perhaps, has been the reaction that it is somehow "creepy" to have everything we browse go into giant databases.[133]

I suggest that this article's analysis of peeping contributes a major insight to the behavioral advertising debate. If there is widespread peeping into the behavioral advertising databases, then that is a big problem. In a world with a lot of peeping, the price of celebrity climbs steeply. Peeping struck candidate Obama for his passport and cell phone records, and Joe the Plumber for becoming prominent in a presidential debate. Going forward, would peeping apply to every website the next candidate or suddenly famous person ever visited?

Writing in 2000, before the current state-of-the-art of behavioral advertising, Jeffrey Rosen in *The Unwanted Gaze* emphasized the problem that one incident could be taken out of context to caricature an individual and harm that person's entire career or reputation.[134] When it comes to web surfing, very many individuals have gone to some site that would be embarrassing or worse if it became known to co-workers, family members, or voters. I submit that a major concern about behavioral advertising is this thus-far-badly-articulated fear of peeping. In a world where a database exists that contains such detailed surfing history, a large portion of us could be harmed by a peeping incident.

As a policy response, effective anti-peeping measures are thus a logical part of whatever form of online advertising develops in the coming years. Technical measures can be put in place, including role-based access, audit

---

131. *See generally* Julie E. Cohen, *A Right to Read Anonymously: A Close Look at 'Copyright Management' in Cyberspace*, 28 CONN. L. REV. 981 (1996); Julie Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161 (1997).

132. Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (2006) (limiting access to records of newspapers and other media); Cable Television Privacy Act of 1984, 47 U.S.C. § 551 (2006) (limiting access to cable television programs viewed by subscribers); *see also* Tattered Cover, Inc. v. City of Thorton, 44 P.3d 1044, 1053 (Colo. 2002) (setting higher standard for discovery of books and other reading material).

133. *E.g.*, Neil Munro, *The Ever-Expanding Network of Local and Federal Databases*, 45 COMM. ACM 17, 17-19 (2002).

134. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

logs, masking of individual identity, and deletion after a relatively short time. Legal and administrative measures can also be implemented, including training, announcement of job sanctions for peeping, and perhaps the notices of peeping discussed above.

For behavioral advertising, it has become technically very complex for an individual to avoid the tracking done in the name of online advertising. When individual choice is difficult to implement, then the challenge is how to build a *system* that protects the individual's interests. Unless the systemic problem of peeping is effectively addressed, then critics of behavioral advertising retain a powerful critique of current practices. We have seen instances of peeping into supposedly sensitive databases such as medical and phone records, so we should not blithely assume it will be absent from the oh-so-interesting databases now being created of every web site that we ever visit.

More optimistically, the risks from behavioral advertising are reduced if we have effective technical and administrative controls against peeping. If the system is trustworthy, then the harms from the databases of surfing are less. It is relatively rare for the government or a litigant to need access to a record, and even rarer for the advertising database to be the subject of a search warrant or subpoena. (Once a police investigation or civil litigation gets started, the prime databases are likely to be a bank or telecommunications provider, rather than advertisers who may have set a cookie to track where a user browsed.)

The recent experience of our political and entertainment celebrities, however, does not support such optimism. Peeping seems increasingly common, and we will need to work much harder to pull down the blinds and otherwise create peace of mind that we will not fall victim to it.

VII. CONCLUSION

Phenomena such as peeping, gossip, and voyeurism are social and psychological issues rather than purely legal ones. With the increasing prevalence of detailed databases, a far larger number of employees can have access to the pictures, reading habits, and activities of politicians, celebrities, neighbors, family members, and anyone else.

Technical and administrative measures that can reduce the incidence of peeping. Probably even more importantly, high-profile examples of peeping should be lessons for our society. The traditional punishment for peeping was blindness for Tiresias and Peeping Tom, and being turned into stone for Lot's wife. The power of these stories is to teach us, or remind us, of the seriousness of the unwanted gaze.