Privacy and Artificial Agents, or, Is Google Reading My Email?

Samir Chopra
Department of Computer and Information Science
Brooklyn College
Brooklyn, NY 11210
schopra@sci.brooklyn.cuny.edu

Laurence White
Rue Franklin 157
Brussels B-1000
Belgium
laurencefwhite@gmail.com

Abstract

We investigate legal and philosophical notions of privacy in the context of artificial agents. Our analysis utilizes a normative account of privacy that defends its value and the extent to which it should be protected: privacy is treated as an interest with moral value, to supplement the legal claim that privacy is a legal right worthy of protection by society and the law. We argue that the fact that the only entity to access my personal data (such as email) is an artificial agent is irrelevant to whether a breach of privacy has occurred. What is relevant are the capacities of the agent: what the agent is both able and empowered to do with that information. We show how concepts of legal agency and attribution of knowledge gained by agents to their principals are crucial to understanding whether a violation of privacy has occurred when artificial agents access users' personal data. As natural language processing and semantic extraction used in artificial agents become increasingly sophisticated, so the corporations that deploy those agents will be more likely to be attributed with knowledge of their users' personal information, thus triggering significant potential legal liabilities.

1 Introduction

Privacy's philosophical history dates back to Aristotle's famous distinction between the public sphere of political activity and the private sphere of domestic life. Philosophical debates since then have distinguished between descriptive (what is worthy of being kept private) and prescriptive (what is of normative value in privacy) accounts of privacy. Of particular interest in this rich discussion [Paul *et. al* 2000; Schoeman, 1984; Agre & Rotenberg, 1997] is the normative concept of *informational privacy*. This notion is increasingly threatened by the colossal amounts of personal information collected as individuals participate in online activities that identify them, and stored in commercial online databases whose access policies may not be sufficiently respectful of individual privacy, or in insecure databases maintained by federal, state, and local governments [Garfinkel, 2004].

Concerns over the violation of privacy by technological advances are not new; the first expression of concern in this regard dates back to 1890. There is a new wrinkle in the landscape however: the collection and use of information by programs such as Google's AdSense scanning technology, which when applied to Google's Gmail system leads to the generation of advertisements (ads) that are relevant to identified keywords in message bodies[1]. Google conducts auctions of each keyword, so that the highest bidders have the right to have their ads linked to that keyword.

Google has sought to assuage concerns over this putative violation of privacy by pointing to *the non-involvement of humans in the process*. In the coming decades, we may expect increasing use of this technology and artificial agents, such as data-miners and bots, which scan online databases for profiling purposes. And we may see an increasing usage of the so-called Google defense: if humans do not read your private communications, your privacy has not been violated. This raises a question for concerned citizens and designers of autonomous artificial agents: to what extent should these agents have access to personal information? Does it matter that a human is not reading my email? Should it concern us that information we would not entrust to a human willingly, citing privacy concerns, is collected, stored and analyzed by 'a mere program'? We will argue that it should; it is the *technical capacities* of this program that are relevant.

The outline of this paper is as follows: in Section 2, we argue for privacy as a moral value; in Section 3 we introduce the general theory of artificial agents and attribution of knowledge to their principals; in Section 4 we address whether Google is 'reading my mail', and in Section 5 we inquire into the legal implications for Google if that is the case. Our conclusions are set out in Section 6.

2 The Value of Privacy

In their seminal 1890 paper "The Right to Privacy", Samuel Warren and Louis Brandeis argued that "political, social, and economic changes" and "the right to be let alone" entailed that the law offer privacy protection to individuals. Responding to technological changes in the media, such as the advent of photography, Warren and Brandeis noted the invasion of privacy brought about by release of details pertaining to a person's private life. They argued that a general

[1] AdSense technology is described in US Patent Applications 20040059712, 20040093327 and 20040167928.

right to privacy would protect the extent to which one's innermost mental life could be shared with others, afford "peace of mind", and be grounded in a general right of immunity of the person, "the right to one's personality" (interpretable as protection of an individual's autonomy). While existent US law offered protection—via the Fourth Amendment—for homes and their interiors against searches, they argued that new, potentially intrusive, technology made it necessary to formalize this protection under the rubric of privacy.

This formulation of the right to privacy is known as "control over information about oneself"; it says nothing about the identity of the agent gaining control over information. Thus, photographs taken by an automated camera mounted outside someone's home entail a loss of privacy even if the photographs had not yet been viewed by humans: the person inside would have had no control over the release of this information. The 'information leakage' would be enough violation of privacy; the violation would take place at the moment the photograph was taken, not when they were viewed. For Warren and Brandeis, the right to privacy is a moral value worthy of protection under law, with no concessions made to contingent violations.

To echo Warren and Brandeis' concerns, three landmark cases established that privacy needed protection from technological invasions. In the first electronic surveillance case, Olmstead v. United States (1928)[2], the US Supreme Court ruled that warrants were not necessary in order for federal agents to carry out phone-taps. The Court ruled that the Fourth Amendment only protected against "physical invasions" by law enforcement officers. Dissenting from the majority, Justice Brandeis argued for a reconfigured notion of privacy to accommodate new technology. In 1967, the Supreme Court overruled this decision in deciding Katz v. United States[3], judging that tapping phone conversations in a public phone booth was a violation of the Fourth Amendment. The court ruled that there is a "reasonable expectation of privacy" in public spaces: "[T]he Fourth Amendment protects people, not places. [What a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Finally, in 1995, a US Military Court, citing the Katz decision, ruled that an individual has a reasonable expectation of privacy in his private e-mail, even if stored and sent using an online service[4]. The right to informational privacy then, has been understood as protecting not just against surveillance, monitoring and warrantless searches, but also against appropriation and misuses of one's communications. Again, these rulings *did not make their judgments contingent upon the nature of the agent that violates a citizen's right to privacy*.

Theorizing since then has reflected this concern with informational privacy[5] and continues to link the notion of personal autonomy to it. [Westin, 1967] describes privacy as the ability to determine for ourselves when, how, and to what extent information about us is communicated to others; while [Parent, 1983] describes privacy as, "the condition of not having undocumented personal information known or possessed by others". Common to these analyses is the notion of the *loss of autonomy* when the agents' privacy is breached; each problematic appropriation of an agent's personal information takes place without his or her consent. Westin's analysis raises the issue of autonomous determination of the release of information, while Parent notes that information may only be released when the individual has itself documented it publicly. These analyses suggest a moral wrong occurs with the uncontrolled, non-autonomous release of information pertaining to an individual.

More recently, [Lessig, 2000] argues that the right to privacy provides a measure of dignity, and tests our intuitions with a hypothetical situation. The US National Security Agency (NSA) releases a worm over the Internet in an effort to try and find a file missing from their servers. This program enters every US resident's computer and scans its hard disk; if it finds the file, it sends a report to the NSA; if not, it moves on. The program is smart enough to only use idle CPU cycles on each machine. No intrusion then, that bothered me, took place; nothing was disturbed; the contents of my hard disk were not reported to the government (even my illegal collection of copyrighted music). An artificial, not human, agent went through my files (only their names, not their contents); no human eyes have seen my data; yet our intuitions pertaining to our sense of dignity and personal autonomy are offended, for we were not asked for permission, our belongings were searched, and we were held potentially suspect until searched. Privacy law finds its foundations in the intuition that we experience moral injury in situations like those in Lessig's example.

Claims for full-blown rights to privacy then, *regardless of the nature of the agent engaged in the violation*, can be understood as carrying normative weight: dignity is a moral good, as is individual autonomy. Understanding informational privacy as an expression of autonomy [Michelfelder, 2001; Scanlan, 2001; Corlett, 2002], and dignity, in addition to viewing it as a constitutional limitation on governmental or corporate power, enables an understanding of it as a moral good, worthy of protection from the assaults of the legal and penal systems, and from changes in technological capacities that increase the potential for the invasive searches of, and the increasing access to, our personal information that artificial agents will come to have. As we will see, when an artificial agent and its principal can be said to 'know' something is crucial in determining whether a breach of privacy has occurred on its accessing our data.

[2] 277 U.S. 438; 48 S. Ct. 564; 72 L. Ed. 944

[3] 389 U.S. 347; 88 S. Ct. 507; 19 L. Ed. 2d 576

[4] *U.S. v. Maxwell*, 42 M.J. 568 (USAF Crim.App. 1995), *rev'd in part*, 45 M.J. 406 (1996). However the mainstream academic assumption is that the Fourth Amendment does not protect email stored by third parties see, e.g., [Schwartz et al, 2005] at p. 602.

[5] See discussions concerning medical data e.g., [Tavani, 2004; Lankshear & Mason 2001].

3 Attribution of Knowledge held by Agents

[Chopra & White 2004, 2005] argued for a development of legal doctrine, whereby artificial agents are assimilated to human agents for the purposes of entering into contracts and for the purposes of accumulating knowledge that could legally be attributed (or 'imputed') to their principals (the legal persons, human or corporate, on whose behalf they act). Artificial agents, on this analysis, would be akin to slaves under Roman law, not legal persons in their own right, but with power to enter into binding arrangements, and receive information, on behalf of their owners, in circumstances where their owners would be bound by those arrangements or that knowledge.

[Chopra & White, 2005] showed that the law of imputed knowledge, whereby the knowledge of a (human or corporate) agent gained within the scope of the agent's employment is imputed to its principal, does not rest on a presumption that the agent has carried out its duty to inform its principal. Rather, they postulate that it is the *ability* of the agent to convey the requisite information to the principal—that knowledge is ready to hand—that is crucial. They further argue that artificial agents, just like human ones, should be considered to be repositories of legally relevant knowledge on behalf of their principals, a compelling approach when most information held by corporations is in the form of electronic records. They suggest a distinction between electronic records, which are ready-to-hand and should be considered to be part of the knowledge of the corporation whether or not any human agent knows their contents, and paper records which the corporation controlling them cannot be presumed to know the contents of, in the absence of a human or artificial agent that does. Attribution then, does not depend on a notional passing of knowledge up the management hierarchy; rather, *attribution of knowledge held by an agent to the principal depends on the functions granted to the agent, i.e., the existence and scope of the agency relationship*.

What of 'horizontal' information barriers, which prevent management from gaining access to the knowledge held by agents lower down the corporate hierarchy? These issues are important in medical situations, where patient confidentiality means that management and others not directly concerned with the patient's clinical care may have no right to particular patients' records. Yet the law will attribute doctors' knowledge to an employing hospital or practice, for instance in the context of a medical negligence case. The fact that knowledge is not ready-to-hand to the *management* does not mean that it is not counted as the *corporation's* knowledge for legal purposes.

Furthermore, the corporation *itself* legally is attributed with that knowledge. If, for example, the employer made a misleading public statement about the number of patients it had treated who had had a certain medical condition, it could not plead in its defense its lack of knowledge of its patients' medical conditions. The proper response would be for the employer to establish a system whereby patient statistics—properly anonymized—would be collected and reported accurately. Hence, knowledge can be attributed from an agent to a corporate principal even when the agent is under an obligation not to convey the knowledge to other agents of the corporate principal.[6]

4 Is Google Reading My Email?

The launch of Gmail was attended by considerable disquiet among commentators to the effect that Google's screening methodology amounted to a breach of the user's privacy. One response was that users are free to give up their own privacy, and are asked to do so on a regular basis, in exchange for receiving certain services. However, Google's response was instructive: *there was no issue of a breach of privacy because humans were not reading the users' mail*:[7]

> **1. Is Google reading my email?**
>
> No. Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do. Google…uses this scanning technology to deliver targeted text ads and other related information. This is completely automated and involves no humans.

However, thirty-one worldwide privacy bodies were quick to point out:[8]

> … a computer system, with its greater storage, memory, and associative ability than a human's, could be just as invasive as a human listening to the communications, if not more so.

We agree with the privacy bodies that the mere fact that humans are not involved is not relevant to either the legal or moral dimensions of Google's behavior. However, the limited functionality of the software agents used to process the mail, and the limits on what is done with the information extracted, gives the user sufficient comfort that intimate details are not available for others to peruse. For many users, including these authors, the trade-offs are worthwhile.

Significantly, Google does not itself place complete faith in the automated nature of the scanning process:[9]

> All major email services…automatically scan email content for the benefit of users. *When email messages are fully protected from unwanted disclosure, the automatic scanning of email does not amount to a violation of privacy*. [emphasis added]… [D]elivering information gathered through email scanning to a third party would be a violation of privacy. Google does not do this. Neither email content nor any personal information is ever shared with other parties...

Google then, implicitly acknowledges that, however automated the process, if details were forwarded on to third parties, a violation of privacy would occur. Thus, Google recognizes that the automated nature of the process, while of comfort to users who are grateful their personal messages are not being read by human strangers, is not a defense to

[6] In this respect, corporate principals may be different than other kinds of principal. See [Langevoort, 2003]

[7] http://mail.google.com/mail/help/about_privacy.html

[8] http://www.privacyrights.org/ar/GmailLetter.htm

[9] http://mail.google.com/mail/help/more.html

the charge of a violation of privacy. Their defense is that no onward disclosure takes place. However, the fact that the software agents cannot do anything more with the information extracted than generate advertisements to place alongside those mails is not, by itself, sufficient to dispel the legal and ethical dilemmas at play.

Right now, Google's system is able to identify users who have an interest—innocent or otherwise—in terrorism, Nazism or child pornography. Many people interested in these topics would have innocent motives, whether they are academics, law enforcement officials or curious citizens. But a small but relatively high percentage (compared with the total user group) would have a less innocent interest. Information of this type is a valuable commodity in a world gripped by fears of terrorism and Internet pedophilia. Google was recently ordered by the US District Court to hand over anonymized information about URLs returned by user searches,[10] and it and other online companies have been asked by the US Justice Department to retain records of users' search queries for as long as two years.[11]

If Google were to find itself the subject of a valid subpoena relating to email content, and the court were to find the request not over-broad, it would be of no comfort to users that no human had read their mail. Google notes that it is subject to authorized requests for information:[12]

> Many of the concerns around Gmail have centered on the use of automatic scanning technology to deliver relevant ads and related information….These concerns are misdirected. *Automatic scanning technology alone does not make it any easier for a government to obtain or access your...private information.* ...Google does…comply with…search warrants, court orders, or subpoenas seeking account information. These same processes apply to all law-abiding companies….[T]he primary protections you have against intrusions by the government are the laws that apply to where you live. [Emphasis added]

Google's assertion emphasized above is questionable. While the huge Gmail databases could be queried under a subpoena using custom-built filters to track down 'bad guys', Gmail's development work is self-evidently eliminating the need to custom-build equivalent filters, and accelerating the development of more sophisticated filters that can build on their functionality.

So, Is Google reading my mail? At present, we conclude not: AdSense software does not currently appear to possess the semantic analysis capacity that we could call 'reading'. We would argue it knows what we are talking about and in some circumstances that may be compromising enough. But it does not, crucially, appear to know what we are saying and what emotions we are expressing about what we are talking about.

Google could however, continue to refine its software's sophistication, so that the semantic content of the mails being scanned becomes increasingly known to the software deployed. Its system might categorize mail according to what the mail was about, and which emotion concerning the subject matter of the email was being expressed. Advertisers might find this useful. More invasively, Google might want to build a profile of users' tastes, habits and characteristics (such as sex, race, religion, income); advertisers would find that kind of information interesting too. When that technology eventuates, it would be natural to say that Google is 'reading' my mail, just as we speak of computers 'knowing' that summer time has started. Intentional attributions in the former case are even more plausible than the latter.

5 Legal Implications for Google

Even if Google could then be said to be 'reading' its users' mail in a loose sense, it would not attain the level of semantic understanding of the mail that a human would. Nevertheless, the fact that Google has *some* (if not complete) knowledge of the contents of its users' emails has potential legal implications, which need to be kept in mind by designers of artificial agents.

Firstly, 'reading' its users' mail could have legal implications for Google under a US and a Californian statute relating to wiretapping. The US Wiretap Act[13] criminalizes a person who "intentionally intercepts" any "electronic communication", subject to certain exceptions[14], and who subsequently uses or discloses the contents of the electronic communication, having reason to know that the information was obtained in violation of the provision[15]. It also provides for civil damages for a person whose electronic communication is intercepted, disclosed, or intentionally used in violation of the chapter.[16]

It has been suggested [Miller, 2005] that Google's deployment of the AdSense technology in its Gmail service could violate the Wiretap Act as the scanning of each email on its first opening would constitute an 'interception' for the purposes of the Act.[17] It could also be argued that its use of the contents of an email by the AdSense program would be a use by a person having reason to know that the information was obtained in violation of the provision, contrary to the statute.

However, there is a specific exception in the Wiretap Act where "one of the parties to the communication has given prior consent to such interception".[18] Google could argue that it is protected by the consent that its users give to its terms of use. But, as [Miller, 2005] points out, Google's terms of use are made known after the user has signed up to the Google account, and its privacy policies, which can be accessed before registration, are not specific on the issue. So, arguably, Google is intercepting its users' emails without their consent. Nevertheless, it seems that its users are

[10] United States v Google, Inc., 234 F.R.D. 674.
[11] http://tinyurl.com/f5u5q
[12] Google Inc., 'More on Gmail and privacy', note 9, *op. cit.*

[13] 18 USC Chapter 119—Wire And Electronic Communications Interception And Interception Of Oral Communications
[14] 18 USC § 2511(1)(a)
[15] 18 USC § 2511(1)(c) and (d)
[16] 18 USC § 2520(a)
[17] *United States v Councilman* (2005) 418 F.3d 67.
[18] 18 USC § 2520(2)(d)

content to trade-off the loss of privacy suffered for the convenience of a capacious, free online email storage system. Implicit consent or consent by conduct might well be found by a court that had to decide the issue. Were the issue to become a critical one Google could review its registration process to ensure adequate consent was obtained.

One privacy interest that is not protected by this conclusion, however, is that of the *sender* of email to a Gmail account. Unless it is assumed that all senders are aware of the details of Google's AdSense software, it seems there would be no protection for the sender of an email to a Gmail account from having her mail 'read' by Google.

Once opened, email retained on the Gmail server may[19] be subject to a separate body of law relating to unauthorized access to stored electronic communications in the facilities of an electronic communications service provider.[20] [Miller, 2005] argues that Google would be in danger of violating this rule. However, even if this body of law is applicable, there are defenses that would be potentially applicable to Google where the conduct complained of is authorized by:

- 'the person or entity providing a[n] … electronic communications service'; or
- 'a user of that service with respect to a communication of or intended for that user'[21].

While [Miller, 2005] argues that the first of these exceptions is too broad, it would seem to be squarely applicable on the law as it stands. Furthermore, Google could argue that it has the authorization of its users to engage in scanning. On this point, the argument about consent set out above would be equally applicable.

California Penal Code § 631 establishes expansive protections for "communications", which includes e-mail messages. This provision establishes a criminal offence where any person:

> …willfully and without the consent of all parties to the communication, or in any unauthorized manner, *reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication* while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, … [emphasis added]

Central to any argument that Google is in violation of the provision is the proposition that Google is 'reading or learning the contents or meaning of any message' within Gmail.

On 3rd May 2004, the Electronic Privacy Information Centre (EPIC) wrote—on behalf of two other privacy organizations and itself—to California Attorney General Lokyer arguing that Google was in breach of §631(a).[22] We agree with the EPIC that Google should be treated as 'learning the contents' of the mails in the Gmail system and therefore in *prima facie* violation of the statute. Further, it appears to be using information so obtained, again in *prima facie* violation of the statute. If the AdSense technology is developed further, Google may violate the prohibition against 'reading' its users' mail. The provision raises a host of legal issues that would need to be demonstrated in practice in order to prove a violation on the part of Google. For example, whether the email was in 'transit' for the purposes of the provision, and whether senders had consented to the application of AdSense technology. In the event, the Californian Attorney-General failed to give any definitive response to the allegations therein.[23]

Leaving aside questions of liability under these particular statutes, there is *the issue of potential liability for knowledge that Google might gain from users' mail*. Let us suppose that Google's AdSense semantic extraction technology continued to be developed. Suppose the system becomes aware, not only of what my email is about, what emotion or attitude is being expressed, but starts to model in detail what is being said. Such a system could become a kind of 'personal assistant', managing my diary and automatically answering some emails. In such a situation we would find it completely natural to say the system was 'reading' my mail. But the knowledge gained by such a system might lead Google to gain 'unwanted' knowledge.

Suppose, for example, that terrorists detonate a weapon of mass destruction in a major city causing great loss of life, that the terrorists used Gmail to plot the attack, and the 'personal assistant' functionality was switched on. Let us also suppose (contrary to current fact) that Google was subject to a law which required all persons (including companies) to report knowledge of intended terrorism to the authorities. (In some jurisdictions, a person who merely *knows* of an intended act of *treason* is required to inform the authorities and commits a crime if she fails to do so; in the US, an additional act of concealment is currently required.[24])

In this scenario, on the legal analysis above, Google could be attributed with knowledge gained by its agent that a terrorist plot had been planned: a failure to warn the authorities of such a plot could, we maintain, be cause for prosecution of Google itself. Furthermore, if Google failed to issue a warning about a planned terrorist attack, the firm might even be sued in a civil action by the families of the dead, by injured survivors and by owners of damaged property, for breach of its statutory duty to warn the authorities.

Thus, if firms such as Google wish to 'read' users' mail, they would (absent shield laws such as are put in place for 'common carriers') need to establish systems whereby suspicious mails are routinely alerted to the police and other authorities. As in the example of medically confidential

[19] There is a body of case law that holds that only an Internet service provider is capable of the provision of an 'electronic communication service' [Goldberg, 2005]. If true, webmail services would not qualify, and the prohibition would not apply.

[20] 18 USC § 2701 *et seq.*

[21] 18 USC § 2701(c)(1) and (2)

[22] See http://www.epic.org/privacy/gmail/agltr5.3.04.html.

[23] See http://www.epic.org/privacy/gmail/caagack.pdf

[24] Criminal Code (Australia) s. 9A(2)(b); this is a crime at common law in the UK. Compare 18 USC § 2382.

information, the fact that the information should not ordinarily[25] be shared with employees of Google does not mean it can not be legally attributed to Google. However, requiring Google to have the capacity to warn of possible terrorist offences would require Google to re-engineer its systems so as to better suit it to a quasi-law enforcement role.

We acknowledge that resolution of the policy question whether this would be justified would depend not only on legal notions of attribution of knowledge, but as well on policy and cost-benefit grounds. It might be resolved in legislatures rather than in courts, given the stakes involved. Such a fundamental policy question would need to be sensitive to issues such as the costs of building such an alert system, whether building such as system would be effectual (given the ability of terrorists to set up email accounts without such intrusive scanning and their access to strong encryption), and so on. One defensive strategy Google might employ would be to design the system in such a way that the 'personal assistant' functionality was *exclusively* the agent of the user and not of Google itself. The law of attribution in cases of dual agency is a very complex area and outside the scope of this paper. We hope to address it in a future work.

6 Conclusion

We have a provided a legal and philosophical analysis of issues regarding access to our personal data by artificial agents and its implications for our privacy. After arguing for the moral value of privacy, we pointed out how the concepts of legal agency and attribution of knowledge gained by agents to their principals are crucial to understanding whether a violation of privacy has occurred. Designers of artificial agents which access users' personal information or private communications need to be mindful of possible privacy implications: the more sophisticated their systems become, the more likely it is that corporations that deploy those agents will be attributed with knowledge of their users' personal information, possibly triggering significant legal liability. As natural language processing and semantic extraction used in artificial agents becomes increasingly sophisticated, it will be harder to use the Google defense; that no humans are involved in 'reading' our email does not mean that our privacy has not been, and can not be, violated.

References

[Agre and Rotenberg, 1997] P. Agre and M. Rotenberg, (Eds.). *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, MA, 1997.

[Chopra and White, 2004] Samir Chopra and Laurence White. Artificial Agents – Personhood in Law and Philosophy. *Proceedings of ECAI 2004*, IOS Press, Amsterdam, Netherlands, 635–639, 2004. .

[Chopra and White, 2005] Samir Chopra and Laurence White. Attribution of Knowledge to Artificial Agents and their Principals. *Proceedings of IJCAI 2005*, Professional Book Center, 1175-1180, 2005.

[Corlett, 2002] Angelo J Corlett. The Nature and Value of the Moral Right to Privacy. *Public Affairs Quarterly*, 16(4):329–350, 2002.

[Garfinkel, 2004] Simson Garfinkel. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly, Sebastopol, 2004.

[Goldberg, 2005] M.A. Goldberg. The Googling of Online Privacy: Gmail, Search–Engine Histories and the New Frontier of Protecting Private information on the Web. *Lewis & Clark Law Review*, 9:249–272, Spring 2005.

[Hollander and Salzedo, 2004] Charles Hollander and Simon Salzedo. *Conflicts of Interest and Chinese Walls (2nd Edition)*. Sweet & Maxwell, London, 2004.

[Langevoort, 2003] Donald C. Langevoort. Agency law Inside the Corporation: Problems of Candor and Knowledge. *University of Cincinnati Law Review*, 71:1187–1231, Summer, 2003.

[Lankshead and Mason, 2001] Gloria Lankshead and David Mason. Technology and Ethical Dilemmas in a Medical Setting: Privacy, Professional Autonomy, Life and Death. *Ethics and Information Technology*, 3(3):225–235, 2001.

[Lessig, 2000] Lawrence Lessig. *Code and Other Laws of Cyberspace*. Basic Books, New York, 2000.

[Michelfelder, 2001] Diane P. Michelfelder. The Moral Value of Informational Privacy in Cyberspace. *Ethics and Information Technology*, 3(2):129–135, 2001.

[Miller, 2005] J.I. Miller. "Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E–mail Privacy Rights. *Hofstra Law Review*, 33:1607–1641, Summer, 2005.

[Paul *et al*., 2000], J. Paul, F. Miller, E. Paul, (Eds.). *The Right of Privacy*. Cambridge University Press, Cambridge, 2000.

[Scanlan, 2001] Michael Scanlan. Informational Privacy and Moral Values. *Ethics and Information Technology*, 3(1):3–12, 2001.

[Schoeman, 1984] F. Schoeman (Ed.). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, Cambridge, 1984.

[Schwartz et al, 2005] Aris Schwartz, Deirdre Mulligan, Indrani Mondal. Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues. *I/S: A Journal of Law and Policy for the Information Society*. 1:597–617, Spring/Summer, 2005.

[Tavani, 2004] Herman T Tavani. Genomic Research and Data–Mining Technology: Implications for Personal Privacy and Informed Consent. *Ethics and Information Technology*. 6(1): 15–28, 2004.

[25] (i.e., in the absence of a duty to inform the authorities)