PEOPLE CAN BE SO FAKE: A NEW DIMENSION TO PRIVACY AND TECHNOLOGY SCHOLARSHIP

M. Ryan Calo[*]

This article updates the traditional discussion of privacy and technology, focused since the days of Warren and Brandeis on the capacity of technology to manipulate information. It proposes a novel dimension to the impact of anthropomorphic or social design on privacy.

Technologies designed to imitate people—through voice, animation, and natural language—are increasingly commonplace, showing up in our cars, computers, phones, and homes. A rich literature in communications and psychology suggests that we are hardwired to react to such technology as though a person were actually present. Social interfaces accordingly capture our attention, improve interactivity, and can free up our hands for other tasks.

At the same time, technologies that imitate people have the potential to implicate long-standing privacy values. One of the well-documented effects on users of interfaces and devices that emulate people is the sensation of being observed and evaluated. Their presence can alter our attitude, behavior, and physiological state. Widespread adoption of such technology may accordingly lessen opportunities for solitude and chill curiosity and self-development. These effects are all the more dangerous in that they cannot be addressed through traditional privacy protections such as encryption or anonymization. At the same time, the unique properties of social technology also present an opportunity to improve privacy, particularly online.

---

[*] Stanford Law School, Center for Internet and Society. JD, University of Michigan 2005. BA, Philosophy, Dartmouth College 1999. Thanks to Mark Lemley, Lauren Gelman, David Ball, and Rony Guldmann at Stanford Law School for a close read of earlier drafts, and to Lawrence Lessig, Jennifer Urban, and Harry Surden for helping me think through the issues. Thanks to Daniel Solove and Chris Jay Hoofnagle for inviting me to workshop this Article at the Privacy Law Scholars Conference at UC Berkeley Law School, Andrea Matwyshyn for presenting the paper, and Michael Froomkin, Danielle Citron, Paul Ohm, and other participations for very helpful comments. Special thanks to the Stanford University Department of Communications for the invaluable guidance, especially Cliff Nass, Victoria Groom, Helen Harris, Daniel Kreiss, and Jesse Fox. Thanks finally to my wife Jean for her great ideas and support.

INTRODUCTION

What if your every Internet search were conducted by a feisty librarian? Ms. Dewey—the virtual host of a search engine run by Microsoft between 2001 and 2006 as part of a marketing campaign—presided over just such an arrangement.[1] Ms. Dewey stood directly behind a simple and familiar search box and greeted users as they arrived at site. A fully rendered video image based on a professional actress, Ms. Dewey would react differently depending on a user's search queries. She displayed other human qualities such as impatience, tapping on the screen with her finger if one waited too long to conduct a search.

Did Ms. Dewey implicate privacy? Like any search engine, Ms. Dewey presumably collected a log of user search queries coupled with an Internet protocol address, time-stamp, and other information.[2] Ms. Dewey may have also collected information on what results users clicked. Microsoft probably stored this information for a period of time and may have shared it with affiliates or law enforcement in accordance with a written policy.[3] Ms. Dewey may also have made it easier to find out information about others; search engines organize and retrieve information it a way that makes it easier to check up on neighbors, job candidates, or first dates.

But Ms. Dewey had another, entirely distinct effect on users—one that has practically nothing to do with the information Microsoft collects, processes, or disseminates. She seemed like person.

Study after study shows that humans are hardwired to react to technological facsimiles like Ms. Dewey as though a person were actually present.[4] Human-like computer interfaces and machines evoke powerful subconscious and physiological reactions, often identical to our reactions to one other.[5] We of course understand the difference between a person and a computer-generated image intellectually. But a deep literature in communications and psychology evidences that our brains "rarely make[] distinctions between speaking to a machine and speaking to a person" at a

---

[1] Msdewey.com is no longer a live website. Screenshots and other information can be found at http://www.msdewey.com/work/ms-dewey-microsoft.

[2] For a recent discussion of the privacy problems associated with search engines, see Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L.R. 1433 (2008).

[3] *See* Microsoft Online Privacy Statement, *at* http://privacy.microsoft.com/en-us/fullnotice.mspx (last visited September 1, 2009).

[4] *See* Part II.B (collecting studies).

[5] *See id.*

visceral level.[6]

As a general matter, the more anthropomorphic qualities—language, voice, face, eyes, and gestures—an interface possesses, the greater our reaction.[7] Ms. Dewey resembled a person in every sense, and hence likely elicited a strong reaction across multiple lines. But such reactions can occur with the slightest indication of intentionality: people name and arrange play dates for their disk-shaped Roomba vacuum cleaners, for instance, and take them on vacation.[8] As some studies recognize, such effects also explain our reactions to technologies that merely *stand in* for a person, as in the case of a visible microphone or camera.[9]

Importantly, among the effects we experience in the presence of a facsimile like Ms. Dewey is the feeling of being observed and evaluated.[10] These effects can lead directly to measurable social inhibitions. Research in communications and psychology has demonstrated, among other things, that introducing a virtual person to a computer interface causes test subjects to disclose less about themselves, "present[] themselves in a more positive light," and even skip sensitive questions on a questionnaire.[11] The presence of eyes alone can lead us to pay for coffee more often on the honor system,[12] or be more charitable in an exercise on giving.[13] These direct and measurable effects occur irrespective of the subject's familiarity with technology, and even where experimenters take pains to explain that no person will ever see the results.[14]

---

[6] CLIFFORD NASS & SCOTT BRAVE, WIRED FOR SPEECH: HOW VOICE ACTIVATES AND ADVANCES THE HUMAN-COMPUTER RELATIONSHIP 4 (2005) (hereinafter "WIRED FOR SPEECH"); Leila Takayama & Clifford Nass, *Driver Safety and information from afar: An experimental driving simulator study of wireless vs. in-car information services*, INT. J. OF HUM.-COMPUTER STUD. 66:3, 173-84 ("These social responses to people and to computers are automatic and largely unconscious.").

[7] *See infra* Part II.

[8] Robert Boyd, *They're gaining on us, but … Even advanced robots fall short of human intelligence,* CHICAGO TRIBUNE, Apr. 23, 2009.

[9] *See, e.g.,* Thomas J.L. van Rompay et al, *The Eye of the Camera: Effects of Security Cameras on Prosocial Behavior*, 41:1 ENVTL. BEHAV. 60-74, 62 (2009) (hereinafter "*The Eye of The Camera*").

[10] *See infra* Part II.B.2 (collecting studies).

[11] Lee Sproull et al, *When the Interface is a Face*, 11 HUM.-COMPUTER INTERACTION 97-124, 112-16 (1996) (hereinafter "*When the Interface is a Face*").

[12] Melissa Batson *et al*., *Cues of Being Watched Enhance Cooperation in a Real-World Setting,* BIOLOGY LETTERS, 2(3):412–14 (2006).

[13] *See* Vanessa Woods, *Pay Up, You Are Being Watched*, NEW SCIENTIST, Mar. 18, 2005 (reporting increase in the presence of a robot picture); Olivia Judson, *Feel the Eyes Upon You*, N.Y. TIMES, Aug. 3, 2008 (reporting increase with computer screen eye spots).

[14] BYRON REEVES & CLIFF NASS, THE MEDIA EQUATION: HOW PEOPLE TREAT

This means that advances in interface design—not just data collection—should matter from the perspective of privacy. Existing and emerging computer interface designs can exert a subtle chill on curiosity, cause discomfort, and even change what people search for or say on the Internet. As in the early days of the telegraph or telephone system,[15] communications transactions may once again be mediated by the functional equivalent of a human operator.

Simulated people affect privacy in an even more basic sense. The mere belief that another person is present triggers a state of "psychological arousal" (and a host of associated behaviors),[16] such that the introduction of voices and faces into historically private spaces could further reduce opportunities for solitude and internality. We place computers and machines into many places where we would not always want humans—for instance, in our offices, cars, and homes. In doing so, we may unwittingly invite the very social inhibitions that form the basis of our decision to exclude others. We could secure fewer and fewer "moments offstage," in Alan Westin's famous words, where we are free to self-define without reference to others.[17]

Ms. Dewey was just a promotion—Microsoft's newest search engine "Bing" does not have an attractive librarian that comments on user searches.[18] But Ms. Dewey is part of a far greater design trend toward making interfaces more salient by imitating people. For a variety of reasons, "[o]ne of the major trends in human-computer interaction … is the development of more natural human-computer interfaces" that present as people.[19] Internet search engines are moving away from a query-to-link interface and toward voice-driven, natural conversation.[20] One example is

---

COMPUTERS, TELEVISION, AND NEW MEDIA LIKE REAL PEOPLE AND PLACES 252 (1996) (hereinafter "THE MEDIA EQUATION").

[15] *See infra* note 40.

[16] *See, e.g.*, Rompay, *The Eye of the Camera* at 62. "Psychological arousal" refers to the absence of relaxation and assurance which corresponds to the presence of others. Sproull, *When the Interface is a Face* at 112.

[17] Alan Westin, PRIVACY & FREEDOM 35 (1967) ("There have to moments 'off stage' when the individual can be 'himself'; tender, angry, irritable, lustful, or dream filled. … To be always 'on' would destroy the human organism.").

[18] *See* http://www.bing.com/ (last visited August 31, 2009).

[19] T.M. Holtgraves et al., *Perceiving Artificial Social Agents*, 23 COMPUTERS & HUM. BEHAV. 2163-2174, 2163 (2007).

[20] *See* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE (2006); Rebecca Corliss, *Interview With John Battelle On The Future of Search*, Hubpot.com (May 12, 2009), *at*

the search engine Weegy, where users can ask questions to a virtual woman with a voice and an animated face;[21] another is the iPhone application Siri, which answers spoken questions and performs tasks like a personal assistant who fits in your pocket.[22]

Human voices and faces are indeed cropping up everywhere, in computers, cars, phones, videos, even bedrooms.[23] GPS devices and mobile phone apps have voices, opinions, and personalities. Websites, including those run by the U.S. government, have virtual hosts; companies have virtual receptionists. The computer giant IBM is testing an entire voice-based Internet, which it refers to as "the Spoken Web."[24]

There is a corresponding trend in personal robotics—a global industry growing at an incredible pace. Many investors—among them Bill Gates—predict that personal robots will be as common in households as personal computers, perhaps within the next few years.[25] Engineers understand that as robots leave the factory floor, they will have to fit in to various human-like roles and spaces, which in turn means resembling people.[26] Indeed, "each new generation of robots is coming progressively closer to simulating human beings in appearance, facial expression, and gesture."[27]

The privacy community is not prepared for this sea change. Technology has always been a key driver of privacy law, scholarship, and policy.[28] Yet

---

http://blog.hubspot.com/blog/tabid/6307/bid/4750/Interview-with-John-Battelle-on-the-Future-of-Search.aspx (last visited November 6, 2009) ("Search is currently an interface for working with machines. As we learn new ways to interact with information, it will stop looking like a list of links and will start feeling more like a conversation.").

[21] *See* www.weegy.com (last visited August 15, 2009).

[22] *See* www.siri.com; John Markoff, *A Software Secretary Takes Charge*, N.Y. TIMES, Dec. 3, 2008.

[23] *See* P.J. Fogg, PERSUASIVE TECHNOLOGIES: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 10 (2003) ("With the growth of embedded computers, computing applications are becoming commonplace in locations where human persuaders would not be welcome, such as bathrooms and bedrooms, or where humans cannot go (inside clothing, embedded in automotive systems, or implanted in a toothbrush).").

[24] *See* John Rebeiro, *IBM Testing Voice-Based Web*, NETWORK WORLD, Sept. 11, 2009, *at* http://www.networkworld.com/news/2008/091108-ibm-testing-voice-based.html.

[25] *See* Bill Gates, *A Robot In Every Home*, SCIENTIFIC AMERICAN, Jan. 2007.

[26] *See infra* Part II.A.

[27] Karl MacDorman & Hiroshi Ishiguro, *The uncanny advantage of using androids in cognitive and social science research*, INTERACTION STUD. 7:3, 297-337, 293 (2006).

[28] As Daniel Solove explains, "The development of new technologies kept concern about privacy smoldering for centuries, but the profound proliferation of new information technologies during the twentieth century … made privacy erupt into a frontline issue around the world." DANIEL SOLOVE, UNDERSTANDING PRIVACY 4 (2008).

our concerns reflect a particular understanding of technology's impact on privacy: technology implicates privacy insofar as it manipulates information. Technology is conceived as an instrument that "provides new ways to do old things more easily, cheaply, and more quickly than before."[29] Where the "old thing" involves collecting, processing, or disseminating information, the technology is thought to implicate privacy.

Internet searches implicate privacy, as discussed, because a company now holds a record of our curiosity or because it is easier to find out information about someone. In this sense, today's call for new thinking about privacy to accommodate technologies as diverse as search engines,[30] ubiquitous computing,[31] or radio frequency identification ("RFID"),[32] is little different from Samuel Warren's and Louis Brandeis's 1890 call to expand tort law to accommodate the ease of image collection occasioned by the recent invention of unposed or "instantaneous" photography.[33]

This understanding no longer suffices. Technologies that introduce the equivalent of people into our homes, cars, computers and mobile devices—places historically experienced as private—threaten our dwindling opportunities for solitude and self-development (the importance of which privacy scholars of all sorts have long maintained).[34] In the commercial context, these features of interface design may accordingly trigger

---

[29] Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, __ STAN. L. REV. __, *7 (2009) (forthcoming).

[30] *See, e.g.*, Tene *supra* note 2 at 1433.

[31] *See, e.g.,* Scott Boone, *Ubiquitous Computers, Virtual Worlds, and the Displacement of Property Rights*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 91, 93-94 (2008) ("Two legal issues presented by the advent of ubiquitous computing are readily apparent. The first is the potential loss of privacy in continuously monitored environments that constantly acquire, store and transmit information about individuals in those environments. The second issue is the loss of Fourth Amendment protections that naturally flow from a combination of the government and the initial loss of privacy."). Ubiquitous computing refers to processors that are embedded into physical spaces and networked together. *Id.* at 100-102.

[32] *See, e.g.*, Julie Maning Magid et al, *RFID and Privacy Law: An Integrated Approach*, 46 AM. BUS. L.J. 1 (2009). Radio frequency identification refers to technology capable of wireless transmission of identifying information. *Id.* at n.1.

[33] Samuel Warren & Louis Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193, 195 (1890) (opening with a concern over "[r]ecent inventions and business methods" such as "instantaneous photography").

[34] Lior Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1736 (2008) ("Privacy theorists have long argued that protecting privacy is essential so that individuals can relax, experiment with different personalities to figure out who they truly are, or develop the insights that will make them more productive citizens.").

consumer protection law. The overuse of these techniques by the government may even implicate the First Amendment's prohibition on excessive chilling effects.[35]

Our tendency to react to social technology as though it were actually capable of observation and judgment also presents novel opportunities to enhance privacy. Privacy scholars and advocates often lament the invisibility of modern data collection.[36] Privacy policies meant to mitigate the problem of notice instead give users, who rarely ever read them, a false sense of reassurance about how their data will be used.[37] By placing an apparent person at the site of data collection, we might use social interfaces to better calibrate a data subject's expectations with the reality of how her information will be used and shared.[38]

This Article makes the case for a new dimension to the impact of technology on privacy. It applies an extensive literature in communications and psychology chronicling our reaction to anthropomorphic designs to an equally rich literature describing the function of privacy in society. In doing so, the Article informs both disciplines by explicitly drawing a connection between the feeling of being observed and the abrogation of privacy by technology. It seeks to focus the privacy and technology debate exactly where it should be—on any misalignment between user experience and actual information practice.

The Article proceeds as follows. Part I discusses the dominant view of technology's impact on privacy. Technology is thought to implicate privacy insofar as it makes it easier, cheaper, or faster to collect, process, or disseminate information. Collection, processing, or dissemination ("CPD")

---

[35] *See Laird v. Tatum*, 408 U.S. 1, 11 (1972) ("In recent years this Court has found in a number of cases that constitutional violations may arise from the deterrent, or 'chilling,' effect of government regulations that fall short of direct prohibitions against the exercise of First Amendment rights.").

[36] Daniel Solove has likened contemporary society to a story out of Franz Kafka: people vaguely realize others are collecting and using their information against them, but lack a sense of what is being collected, when, by whom, or how specifically it is affecting their daily experience. *See* Daniel Solove, *Privacy & Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001). *See also* Daniel Solove, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 6-9 (2004).

[37] *See, e.g.*, Chris Jay Hoofnagle & Jennifer King, *What Californians understand about privacy online*, SSRN Working Paper (Sept. 2008), *at* http://ssrn.com/abstract=1262130; Chris Jay Hoofnagle, *Beyond Google & Evil*, First Monday, Vol. 4-6 (Apr. 2009) at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2326/2156.

[38] *See infra* Part II.B.3.

scholarship proceeds largely by focusing in on one element—collection, for instance—or else by cataloguing the harms caused by greater efficiency and breadth in the manipulation of data.

Part II presents a novel dimension to technology's impact on privacy. It discusses the growing trend toward designing interfaces and machines to present like people. It then leverages an extensive literature in communications and psychology evincing our hard-wired reaction to such technology, which includes the sensation of being observed and evaluated. Finally, Part II links up this literature with privacy scholarship to demonstrate how anthropomorphic design implicates traditional privacy values and may even present a novel opportunity to enhance privacy.

Part III incorporates and applies the insights from Part II by analyzing several existing technologies under a complete framework, and then briefly sketches certain legal ramifications.

Securing privacy in the twenty-first century means more than protecting against a future in which we never *are* alone by controlling the flow of information. We must also account for a future in which we never *feel* alone by recognizing the intended and unintended consequences of how we design our interfaces and machines. Without exploring this new frontier to technology's impact on privacy, we risk silently losing the very societal benefits privacy aims to protect.

I. THE INSTRUMENTALIST CONCEPTION OF TECHNOLOGY

The year was 1976, and artificial intelligence pioneer Joseph Weizenbaum was getting suspicious. Why was the Department of Defense funding as many as four major labs to work on voice recognition technology? "Granted that a speech-recognition machine is bound to be enormously expensive, and that only government and possibly a few very large corporations will therefore be able to afford it," he wondered, "what will [they] be used for?"[39]

When Weizenbaum asked the government, he was told that the Navy wanted to be able to control ships by voice.[40] This struck Weizenbaum as an odd answer. It occurred to him that the most natural government use of voice recognition technology was massive surveillance. "[T]here is no

[39] JOSEPH WEIZENBAUM, COMPUTER, POWER, AND HUMAN REASON: FROM CALCULATION TO JUDGEMENT 272 (1976).

[40] *Id.* at 271.

pressing human problem that will more easily be solved because such machines exist. But such listening machines, could they be made, will make monitoring of voice communications very much easier than it is now."[41]

This insight, that an emerging technology can make some aspect of surveillance "[v]ery much easier than it is now," is important and right, but unfortunately it has come to dominate our thinking about the intersection of technology and privacy. We tend to see technology in a specific way, as an instrument to augment particular human capacities. Technology makes it easier or faster to accomplish certain tasks. Where these tasks include the power to collect, process, or disseminate information, we see the potential for privacy harm.

That we think a certain way about technology is very important. Technology is a—maybe *the*—key driver of privacy law. The standard recital of evidence for this proposition includes Samuel Warren's and Louis Brandeis's reference to the snap camera in formulating the four privacy torts;[42] the evolution of Fourth Amendment jurisprudence in response to wiretapping,[43] dog sniffing,[44] and infrared sensors;[45] the promulgation of and multiple amendments to the Computer Fraud and Abuse Act of 1984[46] and Electronic Privacy Communications Act of 1986;[47] to name but a few. The same is largely true of privacy scholarship: developments in technology are thought to necessitate, or in cases replace, regulation.[48]

---

[41] *Id.* at 272. Weizenbaum continues:

> Perhaps the only reason that there is very little government surveillance in many countries of the world is that such surveillance takes so much manpower. Each conversation on a tapped phone must eventually be listened to by a human agent. But speech-recognizing machines could delete all "uninteresting" conversations and present transcriptions of only the remaining ones.

Id.

[42] Warren & Brandeis, *The Right To Privacy*, at 195.

[43] *See, e.g. Katz v. United States*, 389 U.S. 347 (1967) (extending the Fourth Amendment to cover the wiretapping of individuals in a telephone booth).

[44] *See Illinois v. Caballes*, 543 U.S. 405 (2005).

[45] *See Kyllo v. United States*, 533 U.S. 27 (2001).

[46] 18 U.S.C. § 1030 (2009). The Computer Fraud and Abuse Act was modified in 1986, 1994, 1996, 2001, and again last year.

[47] 18 U.S.C. § 2510 (2009).

[48] *See, e.g.*, UNDERSTANDING PRIVACY at 4 ("[T]he profound proliferation of new information technologies during the twentieth century … made privacy erupt into a frontline issue around the world."); *id.* (referring to Alan Westin's "deep concern over the preservation of privacy under the new pressures of surveillance technology"); JAMES WALDO ET AL, ENGAGING PRIVACY & INFORMATION TECHNOLOGY IN A DIGITAL AGE 2-3,

For all its importance, however, our concept of the relationship between technology and privacy is relatively limited. Technology implicates privacy if it makes it easier or faster (or possible) to collect, process, or disseminate information.

This instrumentalist,[49] information-focused view of the impact of privacy on technology is pervasive. According to Erwin Chemerinsky, "two developments are crucial" with respect to technology's impact on privacy: "First there is unprecedented ability to learn the most intimate and personal things about individuals… Second, there is unprecedented access to information."[50] Orin Kerr observes that "[t]echnology provides new ways to do old things more easily, cheaply, and more quickly than before. As technology advances, legal rules designed for one state of technology begin to have unintended consequences."[51] Ruth Gavison maintains that "[a]dvances in the technology of surveillance and the recording, storage, and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed."[52]

Summarizing the space, Michael Froomkin writes that "Privacy-destroying technologies can be divided into two categories: those that facilitate the acquisition of raw data and those that allow one to process and collate that data in interesting ways."[53] Jonathan Zittrain identifies "three successive shifts in technology from the early 1970s: cheap processors, cheap networks, and cheap sensors. … The third shift has, with the help of

---

28, 88 (2007) (hereinafter "ENGAGING PRIVACY") (listing technology as one of three drivers of privacy change); LAWRENCE LESSIG, CODE 2.0 228-32 (2006) (arguing for a code-based approach to bolstering online privacy); Timothy Casey, *Electronic Surveillance and the Right to be Secure*, 41 U.C. DAVIS L. REV. 977, 984 (2008) ("The modern evolution of the privacy right is closely tied to the story of the industrial-age technological development … Unlike previous technological changes, however, the scope and magnitude of the digital revolution is such that privacy law cannot respond quickly enough to keep privacy relevant and robust."). *See also infra*.

[49] For a discussion of the instrumentalist view of technology, see Maarten Franssen, Gert-Jan Lokhorst, & Ibo van de Poel, *Philosophy of Technology*, in THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta, ed. 2009), *available online at* http://plato.stanford.edu/archives/spr2009/entries/technology/.

[50] Erwin Chemerinsky, *Rediscovering Brandeis' Right to Privacy*, 45 BRANDEIS L.J. 643, 656 (2007).

[51] Kerr, *supra* note 29 at *7.

[52] Ruth Gavison, *Privacy & The Limits of Law*, 89 YALE L.J. 421, 465 (1980). Gavison goes on to note, however, that "[t]echnology is not the whole story." *Id.* at 466.

[53] Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1468 (2000).

the first two, opened the doors to new and formidable privacy invasions."[54]

In 2007, the Committee of the National Research Council faced a sweeping task: map all "potential areas of concern[,] privacy risks to personal information associated with new technologies, [and] trends in technology and practice that will influence impacts on privacy."[55] The committee's many members, including privacy veterans Julie Cohen, Helen Nissenbaum, and Gary Marx, describe holding differing underlying conceptions of privacy.[56] Nevertheless, the committee "found common ground on several points among its members, witnesses, and in the literature. The first point is that privacy touches a very broad set of social concerns related to the control of, access to, and uses of information."[57] According to the report, such "[t]rends in information technology have made it easier and cheaper by orders of magnitude to gather, retain, and analyze information."[58] These are just a few of many examples.[59]

---

[54] Jonathan Zittrain, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT 205 (2007).

[55] ENGAGING PRIVACY at 20.

[56] *Id.* at 84.

[57] *Id.* The report discusses the implication of technology for privacy specifically and at length. It identifies:

> Several trends in technology [that] have led to concerns about privacy. One such trend has to do with hardware that increases the amount of information that can be gathered and stored and the speed with which the information can be analyzed. … A second trend concerns the increasing connectedness of this hardware over networks, which magnifies the increases in the capabilities of the individual pieces. … A third trend has to do with advances in software that allow sophisticated mechanisms for the extraction of information from the data that are stored.

Id. at 88.

[58] *Id.* at 30. *See also id.* at 51 ("Technology can be used to enhance human sense and cognitive capabilities, and these capabilities affect the abililty to collect information"); *id.* at *vii*; (noting that there exist "unbounded options for collecting saving, sharing, and comparing information").

[59] *See, e.g.*, UNDERSTANDING PRIVACY at 189 (noting that often "technology is involved in various privacy problems because it facilitates the gathering, processing, and dissemination of information"); Andrew McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U.L. REV. 63 (2003); Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) ("Modern computing technologies and the Internet have generated the capacity to gather, manipulate, and share massive quantities of data."); Gary Marx, *Seeing Hazily (But Not Darkly) Through the Lens*, 30 LAW & SOC. INQUIRY 339, 377 (2005) ("In addition to the legislative and cultural changes that followed 9/11, means of data collection, storage, analysis, and communication continue to increase in sophistication, power, scale, speed … They also continue to decline in cost."); Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 285 (2003) (paraphrasing others that the major developments that "deeply affect privacy … all concern changes wrought by digital

Privacy and technology scholarship proceeds largely through a process of divvying up the relevant territory. A scholar or set of scholars might focus in on one mechanism—collection, for instance—and explain its particular repercussions for privacy. When people had to pose for photographs, privacy protections around personal images were largely moot. Then "instantaneous" or "unposed" photography made it possible to capture and publish unwanted circumstances, eventually necessitating legal protection. It was once relatively harmless to make court records public because an interested party had to show up at the courthouse or archive. Today, better tools of dissemination like Internet search make for routine perusal of such records.[60]

Again, there are many examples. Acknowledging that "much of the best work on privacy … focuses on issues relating to the storage and reuse of data," Froomkin deals largely with collection in his influential article *The Death of Privacy*.[61] Collection is first in a chain of events that can lead to compromised privacy, Froomkin reasons. Accordingly, "the most effective way of controlling information about oneself is not to share it."[62] Froomkin is concerned that life will become completely open and permeable, particularly to industry and government.[63]

Much of Ian Kerr's work speaks to new technologies that gather information. Kerr has specifically written about the use of software "bots," i.e., low-level artificial intelligence used to gain user trust, but only in order to point out that such techniques allow for the collection of sensitive information on a mass scale.[64] More recent work focuses on the concept of "emanations," essentially a novel way to look at collection.[65]

Privacy scholar and criminologist Gary Marx's recent work *What's New*

---

technology on the ability to manipulate information").

[60] Harry Surden worries, for instance, that search and other technologies of dissemination break down the "structural" protections that privacy enjoys, such as the fact that court records have historically been difficult to access. *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

[61] Froomkin, *supra* note 53 at 1463.

[62] *Id.* at 1464.

[63] *Id.* at 1465.

[64] Ian Kerr, *Bots, Babes, and the Californication of Commerce*, 1 U. OTTAWA L. & TECH. J. 285 (2004).

[65] Ian Kerr, *Emanations, Snoop Dogs and Reasonable Expectation of Privacy*, 52:3 CRIM. L. Q. 392-432 (2007).

About the New Surveillance is broad in scope.[66] Yet Marx too describes the "new" (i.e., contemporary) surveillance largely in terms of its ability to penetrate old barriers to observation:

> New technologies for collecting personal information which transcend the physical, liberty enhancing limitations of the old means are constantly appearing. These probe more deeply, widely and softly than traditional methods, transcending natural (distance, darkness, skin, time and microscopic size) and constructed (walls, sealed envelopes) barriers that historically protected personal information.[67]

Another set of scholars rejects the primacy of collection and focuses instead on processing or retention. According to Tal Zarsky, "mere surveillance … is not grounds for concern, at least not on its own. The fact that there [is] an eye watching and an ear listening is meaningless unless the collected information is *recorded and emphasized*."[68] Zarsky locates the greatest threat posed by technology to privacy is increasingly sophisticated capacity for data mining.[69] He is concerned by "complex algorithms, artificial intelligence, neural networks even genetic-based modeling" capable of drawing incredible and accurate inferences.[70] Such techniques can turn seemingly harmless data into useful intelligence, or take an old database and "discover previously unknown facts and phenomenon."[71]

Still others insist that the full scope of the problem arises only when we see the totality of surveillance capacity, the combined impact of an increased ability to collect *and* process *and* disseminate information.[72]

---

[66] Gary Marx, *What New About the New Surveillance*, SURVEILLANCE & SOC'Y 1(1):9-29 (2005). Marx discusses several aspects of cotemporary surveillance, including its lack of visibility, its continuousness, its difficulty to avoid, and its lower expense. *Id.*

[67] *Id.*

[68] Tal Zarsky, *Mine Your Own Business!: Making the Case for the Implciations of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J. L. & TECH. 1, 4 (2006) (emphasis in original).

[69] *Id.* "Data mining is correctly defined as the 'nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data.'" *Id.* at 5

[70] *Id.* at 6.

[71] *Id.* at 8. *See also* Ira Rubenstein, Ronald Lee, & Paul Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory & Technical Approaches,* 75 U. CHI. L. REV. 261 (2008) (discussing data mining capabilities).

[72] *See* Julie Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029, 2037 (2001) ("More recent commentators have argued that the threat lies not merely in the ease of access to digitized data, but also in the new and more

Richard Clarke coined the term "dataveillance" to describe the systematic observation, collation, and dissemination that modern computing make possible. According to Julie Cohen:

> [T]hreats to privacy from visual surveillance become most acute when visual surveillance and database surveillance are integrated, enabling both real-time identification of visual surveillance subjects and subsequent searches of stored visual information and database surveillance records.[73]

Solove, Cohen, Marx, Paul Schwartz, and others develop sophisticated theoretical models that engage with the impact of existing and emerging technologies on privacy, identity, and autonomy.[74] These accounts identify and complicate the effects of private and public surveillance on the individual or society. For instance, Solove writes about the ability of private and public entities to aggregate data and assemble or share "digital dossiers," and the deep societal repercussions of this capacity.[75]

It is hard to overestimate the importance, interest, and variety of such effects-focused accounts. They have deepened our understanding of the techniques and outcomes of surveillance, potential and actual, for society. Yet these accounts generally proceed from the same starting assumptions about what technologies implicate privacy in the first place and thereby create a problematic state of surveillance—namely, technologies that manipulate data.[76]

A significant minority of commentators plug into the discussion through an exclusive focus on the third element, disclosure of data to others. These

---

complex permutations and profiles that interlinked digital databases enable.").

[73] Julie Cohen, *Privacy, Visibility, Transparency, & Exposure*, 75 U. CHI. L. REV. 181, 183-84 (2008).

[74] *See, e.g.*, DANIEL SOLOVE, THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN A DIGITAL AGE (2004); Paul Schwartz, 52 VAND. L. REV. 1609, 1640-41 (1999); Paul Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000); Julie Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Julie Cohen, *Cyberspace as/and Space*, 117 COLUM. L. REV. 210 (2007).

[75] Daniel Solove, *Digital Dossiers and The Dissipation of the Fourth Amendment,* 75 S. CAL. L. REV. 1083 (2002).

[76] *See, e.g.,* Daniel Solove, THE FUTURE OF REPUTATION 17 (2007) ("We will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world."); Schwartz *supra* note 76 at 1640-41 ("This Article has described a privacy horror show—the widespread collection and disclosure of detailed personal data on the Internet.").

writers deny any privacy harm—or, in the Fourth Amendment context, constitutional implication—unless and until the information gets disclosed to, or is accessed by, a human being. Thus, Richard Parker maintains that "generally, the collection of data by government and other institutions, as described by [Alan] Westin and [Arthur] Miller, is not a loss of privacy per se, but rather a threat to one's privacy."[77] Eric Goldman "question[s] how data mining, without more, creates consequential harm."[78]

This notion features specially in the context of national security. Thought-leaders argue that scanning communications and financial records for evidence of terrorist activity—a.k.a. government data mining—does not invade privacy to the extent it is automated. If anything, such collection and processing by a computer *protects* privacy because no human need ever see the data.[79]

Orin Kerr argues for an "exposure-based approach" to interpreting Fourth Amendment searches of digital files.[80] He subdivides computer forensics into two steps: "the data acquisition phase and the reduction phase."[81] On Kerr's view, "a search occurs when information from or about the data is exposed to human observation."[82] Acquiring the information does not trigger a search, nor is the constitutional test implicated where

---

[77] Richard Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 285 (1973).

[78] Eric Goldman, *Data Mining and Attention Consumption* at 2. Regarding a hypothetical list of male Latino AIDS patients generated by a computer but "not displayed to a human" (instead, "immediately discarded"), Goldman observes:

> Indeed, no adverse consequence of any sort occurs because the world is the same whether the list is generated or not. The data subject does not experience any change, internally (*the data subject never knows that the list was generated*) or externally (*no one else knows either*).

Id. at 4 (emphasis added).

[79] As Richard Posner writes in a popular op ed:

> The collection, mainly through electronic means, of vast amounts of personal information is said to invade privacy. *But machine collection and processing of data cannot, as such, invade privacy.* Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial shifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.

Richard Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005 (emphasis added).

[80] Orin Kerr, *Searchers and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005).

[81] *Id.* at 547.

[82] *Id*. at 551.

information is merely "processed by a computer."[83] Lawrence Lessig also advances the view, albeit with little sympathy, that a government worm that "searches perfectly and invisibly, discovering only the guilty" might fail to trigger Fourth Amendment scrutiny.[84]

In sum, the notion that technology implicates privacy insofar as it augments the power to collect, process, or disseminate information dominates privacy and technology commentary.

The result is that certain assumptions and biases pervade the scholarship. First, technology must manipulate *information* to get on the privacy community's radar. Second, the initial focus is on *the watcher* and her new powers, rather than on the subject of observation and his new detriment. Even where the discussion centers on the complex repercussions of living in a technology-mediated world, these effects are assumed to result from the increased power of observation along established lines.

Scholars—Cohen and Arthur Miller, among others—have noted that generalized surveillance can implicate privacy even in the absence of the collection of information in a specific instance.[85] It is probably enough simply not to know whether you are being watched to experience discomfort or chilling effects;[86] this is of course the exact mechanism

---

[83] *Id.*

[84] LESSIG, *supra* note __ at 20-23. Courts also tend to view the impact of technology in terms of what it allows a human operator to see or do. *See, e.g.*, *United States v. Thomas*, 757 F.2d 1359, 1367 (2d Cir. 1985) (finding that the use of a dog is "not a mere improvement of sense of smell, as ordinary eyeglasses improve vision, but is a significant enhancement accomplished by a different, and far superior, sensory instrument"). *See also Illinois v. Caballes*, 543 U.S. 405 (2005); *Kyllo v. United States*, 533 U.S. 27 (2001); Christopher Slobogin, *Technologically Assisted Physical Surveillance: The American Bar Associations Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 395 (1997) (noting that certain courts have "distinguished between devices that 'improve' human senses and devices that 'replace' them, with the latter being more likely to implicate the Fourth Amendment."). The views espoused by Posner, Kerr, and others have also been contested. *See, e.g.,* Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. 83 (2005).

[85] *Cf.* Cohen, *supra* note __ at 191 ("Even localized, uncoordinated surveillance may be experience as intrusive in ways that have nothing to do with whether data trails are captured."); Gavison, *supra* note 54 at __ ("[A]ttention alone will cause a loss of privacy even if no new information becomes known."); SOLOVE, *supra* note __ at 163 ("Although many forms of intrusion are motivated by a desire to gather information or result in revealing information, intrusion can cause harm even if no information is involved.").

[86] As a small example: customers purchasing certain "awkward" products such as condoms experienced measurably hirer levels of discomfort in experiments when a dummy camera was trained on the register. *See Eye of the Camera* at 69. The camera serves as a

behind Jeremy Bentham's much-discussed design for prisons and other facilities.[87]

Yet the insight that no information need be collected in order for technology to implicate privacy is under-discussed and under-theorized. Privacy harm without collection is seen as a byproduct of a larger surveillance context. The notion that technology and design is evolving in a way that implicates privacy directly by manipulating *experience* instead of *information* is rarely discussed at all. The result is that existing and emerging technologies never make it on the privacy radar. We turn for this evidence to the next Part.

II. A NEW FRONTIER IN PRIVACY AND TECHNOLOGY SCHOLARSHIP

Privacy scholarship of the last century has proven very effective at tracking developments in technology that implicate privacy by manipulating information—that make it easier to collect, process, or disseminate data. Of course, technology evolves in more ways than one. Changes to the architecture and capabilities of everyday devices have been accompanied by equally rapid advances in appearance and user interface design. These design changes may be as or more significant in the ways we experience the world, including with respect to our privacy.

Across a variety of disciplines, sectors, and media, interfaces and machines are becoming more and more human-like in appearance and interaction. Our newest gadgets have faces, voices, or both, and many are capable of understanding a range of natural language commands or inquiries. "People now routinely use voice-input and voice-output systems," observes communications scholar Clifford Nass, "to check airline reservations, order stocks, control cars, navigate the Web, dictate memos into a word processor, entertain children, and perform a host of other tasks."[88] The computers in our cars "are moving from just control under the hood to actively interacting with the driver."[89] The computers on our desktops and phones increasingly present us with "digital communicators" that "autonomously interact with users."[90]

---

reminder of the possibility of surveillance whether or not it was recording, which is sufficient to change individual experience. *Id.*

[87] *See* Jeremy Bentham, THE PANOPTICON WRITINGS (1995). For a seminal discussion of Bentham's Panopticon and its impact on society, see Michel Foucault, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 200 (1979).

[88] WIRED FOR SPEECH at 3.

[89] Takayama & Nass, *supra* note 6 at 1.

[90] Li Gong, *When a Talk-Face Computer is Half-Human and Half-Humanoid: Human*

The phenomenon is also evident in the emerging field of personal robotics—predicted to be a multi-billion dollar industry within five years.[91] Robots developed for home or office use reassemble us more and more. "Each new generation of robots is coming progressively closer to simulating human beings in appearance, facial expression, and gesture."[92] Meanwhile, "the role of assistive agents in the home is becoming more and more important."[93] Robots are falling in price and will soon be widely available outside of standard markets (such as Japan and South Korea).

The upshot of this trend, or set of trends, is that artificial social agents are being introduced into a variety of new contexts—computers, mobile devices, cars, offices, and houses. Psychologists and communications experts will tell you that the effect of this technology on people is unconscious but pronounced, and to an extent unavoidable.[94] We are hardwired to react to these agents as though they were actually human, including with respect to the feeling of being observed and evaluated.[95] Privacy scholars, in turn, will tell you that a key role of privacy is protect a certain measure of solitude and freedom from scrutiny, the absence of which will thwart self-development and encourage conformism.[96]

This Part proceeds as follows. Section A discusses a strong and well-documented trend, that of designing machines and interfaces that present as people. Section B draws from a rich literature around communications and psychology demonstrating that people react to such social entities or reminders as though they were truly human, including with respect to the

---

Identity and Consistency Preference, HUM.-COMPUTER RES. 33, 163-93, 163 (2007).

[91] Nicole Fabris, *Personal Robots Are Here (and by 2015 They'll Be Worth $15 Billion)*, ABI Research (Dec. 2007) *at* http://www.nextgenresearch.com/research/1001344-Personal_Robotics.

[92] Karl MacDorman & Hiroshi Ishiguro, *The uncanny advantage of using androids in cognitive and social science research*, INTERACTION STUD. 7:3, 297-337, 293 (2006).

[93] Siddhartha Srinivasa et al, *HERB: A Home Exploring Robotic Butler*, Intel Working Paper (2009), *1 *at* http://personalrobotics.intel-research.net/projects/herb.php (hereinafter "*HERB*").

[94] *See* Takayama & Nass *supra* note 6 at 2 ("These social responses to people and to computers are automatic and largely unconscious.") The extent of the effect of social technology is not uncontroverted. *See, e.g.* BENJAMIN SHNEIDERMAN, DESIGNING THE USER INTERFACE: STRATEGIES FOR EFFECTIVE HUMAN COMPUTER INTERACTION, (3d 1998) (arguing *inter alia* that anthropomorphized interfaces do not generally succeed and often lead to confusion). There appears to be general agreement, however, that anthropomorphic design elicits reactions in controlled conditions.

[95] *See infra*.

[96] *See infra*.

feeling of being observed. Section C argues that anthropomorphic design accordingly creates two kinds of privacy harms. Introducing apparent agents into the few remaining spaces normally reserved for alone time further threatens solitude, creating a state of constant psychological arousal that many scholars have warned exactly against. Users will no longer be surfing or searching the Internet alone, as it were, with the likely consequence that attitudes and behavior will shift toward the conventional. The final section discusses potential privacy-enhancing uses of anthropomorphic design.

A. The Rise of the Social Interface

A long-term but recently accelerated goal of computer interface designers is to leverage language, voice, and other features of human communication in an effort to make better interfaces. There are several reasons for this trend. People find experiences with social interfaces more engaging, upping human cooperation and making the devices "easier and more comfortable to use."[97] Moreover, voice-activated interfaces allow for hands-free interaction, an increasingly relevant feature as computing follows people wherever they are (for instance, into a car).[98]

It is also getting easier to build good social interfaces. "Advances in artificial intelligence are putting new life into the development of highly interactive and human-like computer-mediated characters or agents. These advances in technology have allowed computer interfaces to become more social and interactive."[99] Although they have been "fairly clunky for a long time," observe human-computer interaction (HCI) researchers, "[d]esigners can aspire to ever more responsive interfaces."[100]

To an even greater extent than in HCI, human-robot interaction is trending toward more social and natural interactions. It is fair to say, along with Victoria Groom, that "the very nature of robots make them appear even more like social entities than most other existing technologies."[101]

---

[97] Lee Sproull et al, *When the Interface is a Face*, 11 HUM.-COMPUTER INTERACTION, 97-124, 98 (2006). *See also infra*.

[98] WIRED FOR SPEECH at 3.

[99] Jong-Eun Roselyn Lee et al, *The Case for Caring Colearners: The Effects of a Computer-Mediated Colearner Agent on Trust and Learning* J. OF COMM. 57, 183-204, 184 (2007).

[100] Sproull *supra* note 97 at 118.

[101] Victoria Groom, *What's the Best Role for a Robot? Cybernetic Models of Existing and Proposed Human-Robot Interaction Strucutres*, ICINCO 2008, 325, *available online at* http://chime.stanford.edu/downloads/groom_robot_role_ICINCO_2008.pdf (last visited

Each new generation of personal robot is more humanlike than the one before.[102] Today's robots "come equipped with the very abilities that humans have evolved to ease our interactions with one another: eye contact, gaze direction, turn-taking, and shared attention."[103]

There are again several reasons behind this trend. One is the widely held belief among roboticists that true intelligence requires a degree of physicality or "embodiment."[104] According to this concept, "to build systems that have human-level intelligence [one must] build robots that have not merely a physical body but a humanoid form."[105] A related position holds that robots will "learn" faster by interacting with people than through rote programming. Cynthia Breazeal, the head of MIT's influential Media Lab, has said of her doctoral project "Kismet," a robot with large, expressive eyes, big floppy ears, and a speaker to make cooing noises: "I hoped that if I built an expressive robot that responded to people, they might treat it in similar ways to babies, and the robot would learn from that."[106] Breazeal's impressive work continues to advance in this direction.[107]

It is also thought that robots must also be "human enough" to accomplish certain tasks or fill certain roles. Roboticists from Carnegie Mellon, for instance, developed a "nursebot" named Pearl for use in hospitals and facilities for the elderly. They found that patients would not respond to Pearl until they made "her" sufficiently human-like; "if the Nursebot is too machine-like, her human clients ignore her, and won't

---

Nov. 8, 2009).

[102] *See* MacDorman & Ishiguro *supra* note 27 at 298.

[103] Robin Marantz Henig, *The Real Transformers*, N.Y. TIMES, Jul. 29, 2007.

[104] H.R. EKBIA, ARTIFICIAL DREAMS 259 (2008). Embodiment refers to placing artificial intelligence in a physical machine capable of sensing and acting upon the outside world. *Id.*

[105] *Id.*

[106] PAMELA MCCURDUCK, MACHINES WHO THINK 454 (2004).

[107] *See, e.g.*, Cynthia Breazeal et al, *An embodied cognition approach to mindreading skills for socially intelligent robots*, INT. J. OF ROBOTICS RES. 28:5, 656-680 (2009). Under the direction of Breazeal, MIT's influential Media Lab has been moving toward ever more lifelike robots. Breazeal pioneers the field of "social robotics" and has helped create a class of "Mobile/Dextrous/Social" robots capable of mimicking emotion and responding to social cues. The Media Lab's newest project, Leonardo, is a collaboration between MIT roboticists and Hollywood animatronics experts at Stan Winston Studio. Leonardo, or "Leo" for short, has a wide range of facial expressions, can gesture naturally, and is responsive to human cues; Leo will, for instance, follow a person's gaze toward a particular object or direction. For more on the MIT media lab, visit http://www.media.mit.edu/.

exercise or take pills."[108] Generally speaking, the more human-like a robot appears, the more we like and respond to it.[109]

As a recent *New York Times* article summarizes:

> The push for social robotics comes from two directions. One is pragmatic: if … the robots are coming, they should be designed in such a way that makes them fit most naturally into the lives of ordinary people. The other is more theoretical: if a robot can be designed to learn in the same way natural creatures do, this could be a significant boost for the field of artificial intelligence.[110]

At any rate, the result is clear: computers and machines that present like people rapidly become the norm. The absence of such an interface may one day mark the exception. Social agents are cropping up in a wide variety of spaces—computers, cars, mobile devices, even our homes. What follows are some examples of the devices that have already been designed and deployed.

1. Computer interfaces, generally.

Americans spend at lot of time at the computer,[111] where they are encountering a slew of virtual agents. "Computer-generated characters are increasingly used as digital communicators on Web sites and in computer applications and games."[112] There are many examples: Microsoft's

---

[108] *See* MCCURDUCK *supra* note 106 at 467. Conversely, researchers worried that by making Nursebot *too* humanlike, patients might form unnatural attachments to it. *Id.*

[109] Henig *supra* note 103 at 10. *See also* Tim Hornyak, *Android Science*, Scientific American, May 2006 *available online at* http://www.sciam.com/article.cfm?id=android-science ("'Appearance is very important to have better interpersonal relationships with a robot,' says the 42-year-old Ishiguro. 'Robots are information media, especially humanoid robots. Their main role in our future is to interact naturally with people.'"). There is a limit to this principle sometimes referred to as the "uncanny valley." Many find a robot that looks quite a lot, but not exactly, like a person quite disconcerting. *See* MacDorman & Ishiguro *supra* note 27.

[110] Henig *supra* note 103 at 3. *See also* Selma Sabanovic, *Robotics in the Wild: Observing Human-Robot Social Interaction Outside the Lab*, 2006 IIEE ("Social robotics projects vary greatly in their stated scientific, technical, and social goals. Some researchers … seek to improve the quality of human-machine interaction by creating interfaces that will rely on social cues and therefore be more natural, intuitive and familiar for users.").

[111] U.S. Census Bureau, *Computer and Internet Use in the United States*, Current Population Reports, Oct. 2005.

[112] Gong & Nass *supra* note 92 at 163.

famously annoying paper clip assistant pops up by default to guide new users of Microsoft Word. An anthropomorphic dog assists computer searches in Microsoft's dominant operating system. A virtual trainer on the popular Wii gaming system encourages exercisers and is able through the Wii controller to detect and react when users are flagging.[113]

The company Active Buddy Inc. creates sophisticated, text-based virtual marketers that operate via instant messenger.[114] ELLEgirlBuddy, developed to promote Elle Girl magazine and its advertisers, interacted with thousands of teens across the Internet before it was eventually retired.[115] Although it had no body, the bot claimed to have body image problems.[116] It was newly developed but claimed to be sixteen.[117] It said it had a "major crush" on its kickboxing instructor.[118] Bots participate regularly on massive multiplayer online games and even Twitter, a text-based social network that is growing exponentially. Such text-based bots are getting so good at faking people that in a recent Turing Award competition,[119] a German program called El Bot fooled three out of four judges into believing it was a person.[120]

The U.S. government has even entered this space. SGT Star is the U.S. Army's virtual recruiter who resides on the website www.GoArmy.com.[121] SGT Star appears as an avatar, speaking out loud in addition to displaying text. He addresses prospective recruits by name (having asked for it). He can be both funny and agitated, as when in response to a command to do push ups he raises his voice to yell, "Hey, I'm the sergeant here. YOU drop down and give me twenty. I can't hear you!" He can also take a compliment; if you tell SGT Star that you like him he responds "Thanks. I try."

---

[113] *See* http://www.nintendo.com/wiifit (last visited Nov. 8, 2009).

[114] *See* Gwendolyn Mariano, *Active Buddy lets companies control bots*, CNET, Feb. 6, 2002 *at* http://news.cnet.com/ActiveBuddy-lets-companies-control-bots/2100-1023_3-830620.html.

[115] I owe this example to Ian Kerr, who uses it in the context of surreptitious data collection. *See* Kerr, *supra* note __ at 313-16.

[116] *Id.* at 313.

[117] *Id.*

[118] *Id.*

[119] The reference is to Alan Turning, the artificial intelligence pioneer that established a test for intelligence based on the computer's ability to appear indistinguishable from a person. *See* Ekbia *supra* note 100 at 18.

[120] Melissa Lafsky, *How Can You Tell If Your IM Buddy Is Really A Machine?*, DISCOVER, Mar. 23, 2009 *available online at* http://discovermagazine.com/2009/mar/25-how-can-you-tell-if-your-im-buddy-is-really-a-machine.

[121] To chat with Sergeant Star, visit www.goarmy.com/chatwithstar.do.

A recent call for research regarding artificial agents by the Department of Advanced Research Projects (DARPA) goes much further, seeking "a highly interactive PC or web-based application to allow family members to verbally interact with 'virtual' renditions of deployed Service Members."[122] The call for research banks on the inability of children to distinguish between a video rendition of their parent and the actual parent. It continues:

> The challenge is to design an application that would allow a child to receive comfort from being able to have simple, virtual conversations with a parent who is not available "in-person." … The child should be able to have a simulated conversation with a parent about generic, everyday topics. For instance, a child may get a response from [from a virtual parent] saying "I love you," or "I miss you," or "Good night mommy/daddy." [123]

2. Internet search in particular.

Search is the gateway to many Internet users' experiences; it too is trending toward the anthropomorphic. Today, search proceeds through a relatively simple process, at least from the perspective of the user: one enters relevant words into a text field and gets back a series of links on a results page. This is very likely to change. According to Marissa Mayer, vice president for search of the dominant search titan Google, "search is in its infancy."[124]

Both of the major ways in which search will change over the next few years implicate anthropomorphic design. First, searches will increasingly occur by voice instead of text. Second, search inquiries and results will increasingly take the form of a natural conversation between the user the interface, rather than a query-to-links transaction.

In a recent interview, Google's Mayer noted that one of the more interesting directions of search will be a shift toward asking questions out loud.[125] Writing on the subject of Google's voice-driven search

---

[122] *See* Department of Defense, Small Business Innovation Research (SBIR), Interactive Topic Information System, Topic Number OSD09-H03, *at* http://www.dodsbir.net/Sitis/archives_display_topic.asp?Bookmark=34653.

[123] *Id.*

[124] Michael Arrington, *Marissa Mayer at Le Web: The (Almost) Complete Interview*, TechCrunch, Dec. 10, 2008 *at* http://www.techcrunch.com/2008/12/10/marissa-mayer-at-le-web-the-almost-complete-interview/.

[125] *Id.*

application, *New York Times* writer John Markoff observes: "The ability to recognize just about any phrase from any person has long been a goal of artificial intelligence researches looking for ways to make man-machine interfaces more natural."[126]

Relatedly, search will move from a transaction between text queries and link results, to a *conversation* between user and software. Weegy is a website where users ask a question of a fully animated human face and receive the answer spoken out loud.[127] The new Wolfram Alpha "answer" engine is more standard in its interface but also takes a natural language interface approach to search.[128] Rather than process key words and churn out a list of results, Wolfram takes sentence-long questions and presents answers in a table. According to its creator, Wolfram is "rather like an expert"; the engine "will understand what you are talking about, do the computation and present to you results."[129] Statements by Google principals indicate that the company is also moving in this direction, toward what is "obviously artificial intelligence" in the sense that it searches and answers with something like a human understanding.[130]

As John Battelle, the author of *The Search*, has said, we will soon look to Internet search like a personal expert.[131] Researchers and designers ultimately imagine a world in which "users will not simply talk *at* and listen *to* computers, nor will computers simply talk *at* or listen *to* users. Instead, people and computers will cooperatively *speak with* one another."[132]

3. Mobile and in-car devices.

We carry increasingly complex devices outside of the home as well—particularly in our cars and mobiles devices. A survey of experts conducted by the Pew Internet and American Life Project predicted that the mobile device will become our primary means to connect to the Internet within 11

---

[126] John Markoff, *Google Is Taking Questions (Spoken, via iPhone)*, N.Y. TIMES, Nov. 14, 2008.

[127] Weegy can be found at www.weegy.com.

[128] Wolfram Alpha can be found at http://www.wolframalpha.com/.

[129] Stephen Shankland, *Google Crashes Wolfram Alpha Debut Party*, CNET, Apr. 28, 2009.

[130] *See, e.g.*, Google Founders Artificial Intelligence Quotes Archives, *at* http://ignoranceisfutile.wordpress.com/2008/09/13/google-founders-artificial-intelligence-quotes-archive/ (collecting quotes from Google principals).

[131] *See supra* note 20.

[132] WIRED FOR SPEECH at 184.

years.[133] To an even greater extent than personal computers, mobile devices leverage voice and natural conversation in an effort to assist "hands free" interactivity. Again, a common function is mobile Internet search. "[U]sers of Google's new mobile application "can place the phone to their ear and ask virtually any question, like 'Where's the nearest Starbucks?' or 'How tall is Mount Everest?'"[134]

Another popular function is hands free feature control. Providers such as vlingo offer voice interfaces to control most aspects of a phone, including data retrieval.[135] Yet another is notification or motivation. Japanese businessmen can purchase "virtual wives," for instance, that appear on their phones and, according to (somewhat objectionable) descriptions on the product, "nag" them to eat healthier.[136] There is a phone application with an avatar that encourages users to do pushups, in part by yelling at them.[137]

Some combine multiple functions: Siri, a mobile application developed using artificial intelligence from the Defense Advanced Research Project Agency ("DARPA").[138] "Like a real assistant, Siri helps you get things done. You interact with Siri by just saying, in your own words, what you want to do."[139] Siri can help you search for and purchase movie tickets, for instance, and share information with friends, all through voice command.

Particularly in the West, individuals spend a significant portion of their time in cars.[140] One report puts average American car time at over 500 hours a year.[141] And, of course, car devices were among the first to imitate people. GPS devices have long relied on voice output, a powerful anthropomorphic force. Many cars have built in navigation devices with programmable personalities and voices. Today's—and certainly tomorrow's—vehicles are "actively interacting with the driver,"[142] such that drivers have something the brain thinks of as a companion. MIT recently

---

[133] Lee Raine & Jan Anderson, *The Future of the Internet III*, Pew Internet & American Life Project, Dec. 14, 2009 *at* http://www.pewinternet.org/Reports/2008/The-Future-of-the-Internet-III.aspx.

[134] Markoff *supra* note 126.

[135] For more on vlingo, go to www.vlingo.com.

[136] This product can be found at http://www.metaboinfo.com/okusama/ (in Japanese).

[137] *See* Mike Butcher, *PushUpFu turns iPhone into fitness gaming network*, TechCrunch Europe, Jan. 2, 2009, *at* http://uk.techcrunch.com/2009/01/02/pushupfu-turns-iphone-into-fitness-gaming-network/.

[138] For press coverage of Siri, see http://www.siri.com/news.

[139] About Siri *at* http://www.siri.com/company.

[140] Stephen Phillips, *The Future Dashboard*, FIN. TIMES, Jun. 4, 2001.

[141] *Id.*

[142] Takayama & Nass *supra* note 6 at 1.

announced plans to build a robotic driving companion.[143]

4. Robots in the home.

Whether in five years or fifteen, the field of personal robotics is poised to explode.[144] Microsoft founder Bill Gates claims that robotics today is at the point personal computing was in the 1970s and guesses that personal robots will one day be as popular and widespread as PCs.[145] According to Gates, "they could have just as profound an impact on the way we work, communicate, learn, and entertain ourselves as the PC has had over the past 30 years."[146]

The numbers are beginning to bear out Gates's prediction. Robots are getting cheaper—having dropped 80% in cost since 1990—and global demand for robots is rising.[147] Business consultant ABA Research predicts that personal robotics will be a 15 billion dollar market by 2015, a number supported by UN commissioned statistics.[148] The government of South Korea, for instance, has announced a goal of one robot per household by 2013.[149]

As noted robot expert and University of Sheffield professor Neil Sharkey explains:

> We are at the crossroads of a brave new world of robotics with the density of robots on the planet picking up year

---

[143] Clay Dillow, *MIT Introduces a Friendly Robot Companion for Your Dashboard*, PopSci, Oct. 29, 2009, *online at* http://www.popsci.com/technology/article/2009-10/friendly-robot-companion-your-dashboard (last visited Nov. 6, 2009).

[144] "Personal" or "service" robotics refers to robots that co-exist with people outside of an industrial context such as a car manufacturing plant. Purposes include customer and personal service, entertainment, and security. MCCURDUCK *supra* note 106 at 467

[145] Gates *supra* note 25 at *2.

[146] *Id. See also* MCCURDUCK *supra* note 106 at 467 (noting a rise in personal and service robotics); Noel Sharkey, *2084: Big robot is watching you: Report on the future of robots for policing, surveillance, and security*, Working Paper, *available online at* http://www.dcs.shef.ac.uk/%7Enoel/Future%20robot%20policing%20report%20Final.doc (hereinafter "*Big Robot*").

[147] *Big Robot* at 3.

[148] *See* Fabris *supra* note 93; Gundren Litzenberger, *The Robots are coming!*, IFR Statistical Department, Press Release, Oct. 23, 2007 (announcing results of the UN 2007 World Robotics Survey); *Greying Japan plans robonurses in five years*, Agence France-Presse, Mar. 3, 2009 ("The trade ministry expects Japan's robotics market to grow to 6.2 trillion yen (63.5 billion dollars) in 2025 from 70 million yen last year.").

[149] *Big Robot* at 3.

> upon year at an increasing rate. The UN robotics survey at the end of 2006 estimated a worldwide operational stock of 3.8 million. A big surprise is that 2.9 million of the robots are for servicing [] personal and private needs. More than a million of these were for leisure and personal entertainment. This is a big change.[150]

Personal robots are already turning up in dozens of private and public contexts. Robotic toys are immensely popular.[151] In Japan, robots assist clothing shoppers.[152] The Tokyo University of Science has had a robotic receptionist in its lobby for several years. According to press coverage of a recent conference on robotics and business, "companies demonstrated a robot firefighter, gardener, receptionist, tour guide and security guard."[153] The computer chip manufacturer Intel "has developed a mobile robot called Herb, the Home Exploring Robotic Butler. Herb can recognize faces and carry out generalized commands such as 'please clean this mess.'"[154]

B. The Media Equation

Social devices are cropping up everywhere; these devices have a measurable effect on people. Specifically, we tend to react to human-like machines and programs as though they were actually human. As this section documents, our brains often cannot tell the difference between fake people and real ones—even though we know, intellectually, that the "person" we're interacting with is not complete or real. We still react to it the same way, right down to our physiological response.[155]

According to the prevailing explanation, humans are over-attuned to other people so as to maximize the evolutionary advantage of society.[156]

---

[150] *Id.*

[151] The Toys R Us "hotlist" for 2009, for instance, is overwhelmingly comprised of robotic toys. *See* http://www.toysrus.com/family/index.jsp?categoryId=3813602 (last visited Nov. 15, 2009).

[152] Danielle Demetriou, *Robot shopping assistants help shoppers in Japan*, Telegraph, Dec. 3, 2008, *at* http://www.telegraph.co.uk/news/worldnews/asia/japan/3541568/Robot-shopping-assistants-help-shoppers-in-Japan.html.

[153] Robert Boyd, *Advantage: Robots*, THE PHILADELPHIA INQUIRER, Apr. 27, 2009.

[154] *Id.*

[155] *See, e.g.*, M. Slater *et al*, *Analysis of physiological responses to social situations in an immersive virtual environment*, PRESENCE: TELEOPERATORS & VIRTUAL ENVIRON. 9, 37-51 (2006).

[156] *See* EKBIA *supra* note 100 at 310; Jane Walker et al, *Using a Human Face in an Interface*, HUM. FACTORS IN COMPUTING SYS., Apr. 24-28, 1994, 85 ("Infants are born with information about the structure of faces; at birth infants exhibit preferences for face-like

Moreover, we evolved at a time when anything that looked human *was* human, and our brains are still hardwired to see the world that way.[157] The ability to manipulate symbols, the presence of eyes, voices, or gestures, and the appearance of self-directed movement all trigger a powerful recognition response, little mitigated by the intellectual awareness that we're dealing with an object. In short, "people are not evolved to twentieth-century technology. The human brain evolved in a world in which *only* humans exhibited rich social behaviors, and a world in which *all* perceived objects were real objects."[158]

One can be skeptical of the exact mechanism, but there is enormous evidence of the phenomenon itself within multiple disciplines. Reactions to social machines and other proxies for people (like cameras or microphones) have been methodically tested by psychologists, sociologists, and others interested in human-machine interaction. They range from simple psychological arousal, i.e., the state of being alert to the presence of another, to measurable changes in behavior and reported attitude. They are often subconscious and occur irrespective of our familiarity with technology. And they include the feeling of being observed or evaluated.

1. Computers as social actors.

Computer scientists working in artificial intelligence have long referred to the "ELIZA effect," after Weizenbaum's computer program designed to mimic psychoanalysis by engaging users in a credible dialogue using the "Rogerian technique of encouraging patients to keep talking."[159] ELIZA asked users text-based questions and, where it did not have an adequate response, inserted ambiguous fillers such as "I see" or "interesting" or "go on."[160] The ELIZA effect refers to the perception by observers that an AI program that mimics people is "smarter" or more complex than its

---

patterns over others."); MacDorman & Ishigaru *supra* note 27 at 318-19 ("*Homo sapiens* may have a genetic predisposition for recognizing faces, [further] honed by expertise developed over a lifetime. … Regardless of its origins, however, *human expertise with hands, faces, and facial expressions is automatically applied to expressive machines that closely resemble people.*") (emphasis in original).

[157] THE MEDIA EQUATION.

[158] *Id.* at 12. *See also* WIRED FOR SPEECH at 3 ("[O]ver the course of 200,000 years of evolution, humans have become voice-activated with brains that are wired to equate voice with people and to act quickly on that identification. … In fact, humans use the same parts of the brain to interact with machines as they do to interact with humans."); Woods *supra* note 13 ("We can manipulate altruistic behavior with a pair of fake eyeballs because ancient parts of our brain fail to recognize them as fake.").

[159] WEIZENABUAM *supra* note 39 at 3; EKBIA *supra* note 100 at 3.

[160] WEIZENABUAM *supra* note 39 at 3.

programming would suggest.[161] According to Weizenbaum, it was his concern over how human users seemed to over-bond with ELIZA that prompted him to write the scathing critique of artificial intelligence discussed in the previous Part.[162]

Communications scholars in a certain mold have developed an entire sub-discipline devoted to the study of how people react to machines, known as "computers as social actors theory" or ("CASA").[163]

> Though computers have been thought to be merely a medium through which communications are transmitted, the CASA theory proposes that people actually engage in the same kinds of social responses that they use with humans. This theory is also supported by numerous experiments on computer voice interfaces. These social responses to people and to computers are automatic and largely unconscious.[164]

CASA pioneers Clifford Nass and Byron Reeves relay years of research in the influential 1996 book, *The Media Equation*.[165] Their method consists largely of reproducing experiments concerning known human behaviors toward other humans and then substituting computer agents for one set of people.[166] In this way, Reeves and Nass show that computers that evidence social characteristics have a similar, or, in some case, the exact same, effect on humans. Computers programmed to be polite, or to evidence certain personalities, have profound effects on the politeness, acceptance, and other behavior of test subjects.[167] Humans respond to flattery and criticism from computers, and rate their experiences with computers more highly if the computer has a similar 'personality' (e.g., submissive) to their own.[168] The results applied to people of all ages and of diverse backgrounds, including those with a familiarity with technology.[169]

Experiments and studies have reinforced and expanded the argument of *The Media Equation*. One team ran experiments where subjects played a

---

[161] EKBIA *supra* note 100 at 357.
[162] WEIZENABUAM *supra* note 39 at 3.
[163] Takayama & Nass *supra* note 6 at 2.
[164] *Id.*
[165] THE MEDIA EQUATION.
[166] *Id.* at 14.
[167] *Id.* at 24.
[168] *Ibid.*
[169] *Id.* at 252.

version of a prisoner's dilemma with a computer.[170] The optimal result required cooperation in the form of successful promise-keeping.[171] Some subjects played with a text-based interface that presented like a standard personal computer; the other played with an interface that looked and acted like a person complete with a face and voice.[172] The experimenters found that "participants kept their promises significantly more with the human-like interface agent."[173] "Cooperation increased when people 'talked' with their interface agent, i.e., discussed their common situation with it, before privately choosing whether or not to cooperate"[174] The use of sufficiently human-like interfaces "led to cooperation rates statistically indistinguishable from cooperation with a real human being."[175]

The phenomenon has also been tested within the field of robotics. Indeed, observes human-robot interaction student Victoria Groom, "[r]obots generally demonstrate even more human characteristics than [computers]… The very nature of robots make them appear even more like social entities than most other existing technologies and elicit an even more powerful social response."[176] "'People become emotionally attached' to robots, [claims] Paul Saffo, a technology forecaster at Stanford University. Two-thirds of the people who own Roombas, the humble floor-sweeping robots, give them names, he said. One-third take their Roombas on vacation."[177]

The more human-like the machine or interface, moreover, the greater the reaction. Canvassing the literature on human robot interaction, informatics professors Karl MacDorman and roboticist Hiroshi Ishiguro conclude that "[h]umanlike appearance and behavior are required to elicit the sorts of responses that people typically direct toward one another," and that "the more humanlike the robot, the more human-directed (largely subconscious) expectations are elicited."[178] In one cited study, test subjects exhibited greater unconscious eye contact behaviors (fixating on the right eye, typical of human-human interaction) when engaging with more

---

[170] S. Parise *et al*, *Cooperating with life-like interface agents*, COMPUTERS IN HUM. BEHAVIOR 15, 123-42 (1999). The prisoners dilemma refers to a hypothetical scenario wherein two or more prisoners are being held separately and asked to inform on one another. Their best case scenario involves staying quiet (i.e., cooperation).

[171] *Id.* at 123-24.

[172] *Id.*

[173] *Id.* at 135.

[174] *Id.* at 124.

[175] *Id.* at 135.

[176] Groom *supra* note 101 at 325.

[177] Boyd *supra* note 151.

[178] MacDorman & Ishiguro *supra* note 27 at 309.

humanoid robots. In another, Japanese subjects only averted their gaze (a sign of respect) when engaging with human-like machines.[179] Groom also notes that "[t]he fewer and weaker the cues of social identity, the lesser the likelihood that a robot will elicit a social response."[180]

2. The feeling of being observed and evaluated.

Importantly, the human response to social design also includes the feeling of being observed and evaluated. Scholars have "documented that people change how they present themselves when interacting with human-like interface agents in comparison with a text interface."[181] Specifically, people "present[] themselves in a more positive light and modif[y] how much they reveal[] about themselves."[182] They also give more, cheat less, and perform differently on skill tests.

One study in the CASA tradition began with the observation that the "mere presence of another human being can influence a person's behavior substantially."[183] It creates a condition of psychological arousal[184] that "leads people to attend more to the social situation and may increase evaluation apprehension and task motivation. … The presence of other people generally also leads people to present themselves in a positive light."[185] For instance, face-to-face interviews "elicit fewer reports of socially undesirable behavior" than other interview methods.[186]

Based on this well-grounded assumption, the team designed a computer-based experiment around a number of hypotheses. First, they postulated that "[p]eople will present themselves in a more positive light when interacting with a talking-face display than when interacting with a text display."[187] Second, they postulated that "[p]eople will be more guarded in their revelations to a talking-face display than to a text display."[188]

Their experiment confirmed these hypotheses. Subjects were told that

---

[179] *Id.* at 316.
[180] Groom *supra* note 101 at 326.
[181] Parise *supra* note 123.
[182] *Id.*
[183] Sproull *supra* note 97 at 101.
[184] The authors define arousal as "a measure of relaxation and assurance." *Id.* at 112.
[185] *Id.* at 98.
[186] *Id.* at 101.
[187] *Id.*
[188] *Id.* at 102.

they were to test a new career guidance computer program consisting of a survey and report. Half of the subjects were given a standard text-based interface, the other an interface that spoke out loud and looked like a person. Throughout the experiment, the team took pains to "ensure that subjects knew that the face was simulated and that no real human being would see their responses" and found evidence that their efforts in this regard were successful.[189] Nevertheless, students in the "face condition" were more aroused, presented themselves more positively, and offered less in response to the counselor program's questions than those in the text condition. They also took longer to respond and skipped particular parts of the survey, suggesting to the team that "they were avoiding certain personal questions."[190]

Raoul Rickenberg and Byron Reeves conducted a study of how introducing an animated character affected individuals as they performed problem-solving tasks on two websites modeled on those of Charles Schwab and Dell Computer.[191] Some subjects performed the tasks with no animated character present, others with an "idle" character at the bottom right of the screen that "generally appeared to be preoccupied with reading a book."[192] A third set of subjects performed the tasks with a character that appeared to take an interest in their every move.

Rickenberg and Reeves found that the mere presence of the idle character raised levels of user anxiety, but that anxiety was most pronounced where the character appeared to be monitoring the subject. They also found that subjects were able to perform fewer tasks in the monitored condition than in either the idle or no character scenario. Interestingly, subjects reported "trusting" the websites more when the character was present, and the most when the character monitored them.[193]

In yet another study, Catherine Zanbaka and her colleagues at UNC Charlotte tested the effect of placing a person or a projection of a virtual person in the same room as a subject performing simple and complex math.[194] They found that participants performed significantly better overall

---

[189] *Id.* at 117.

[190] *Id.* at 113.

[191] Roaul Rickenberg & Byron Reeves, *The Effects of Animated Characters on Anxiety, Task Performance, and Evaluations of User Interfaces*, CHI LETTERS 2:1, Apr. 1-6, 2000.

[192] *Id.* at 52.

[193] *Id.* at 55.

[194] Catherine Zanbaka et al, *Social Responses to Virtual Humans: Implications for Future Interface Design*, CHI 2007 Proceedings: Social Influence, Apr. 28-May 3, 2007.

when they were alone than in the presence—perceived or actual—of another person. Subjects performed simple tasks faster in the presence of others and harder tasks more slowly and with a higher error rate. The researchers found no statistically significant difference between the effect of a real person over a virtual one.[195]

Other experiments with anthropomorphic design have yielded similar results. Terry Burnham and Brian Hare of Harvard University, for instance, invited 96 volunteers to play a computer game in which subjects could choose anonymously to donate money or withhold it.[196] By introducing a mere screen photo of Kismet, the robot designed by Breazeal to elicit a social reaction in humans, Burham and Hare increased donations by thirty percent.[197] In another experiment around donation, subjects consistently donated more where the computer terminal they were using had eyespots on its screen.[198] In yet another study published in *Biology Letters*, UK psychologists found that the presence of a picture with eyes above the collection bin led people to pay for coffee on the honor system far more often than a picture of flowers.[199]

Technology need not itself be anthropomorphic, in the sense of appearing human, to trigger social inhibitions; technologies commonly understood to *stand in* for people as a remote proxy tend to have the same effect. Recent research has shown, for instance, that "[t]he mere presence of a security camera … may not only inhibit unwelcome behaviors but also have an effect on the extent to which people demonstrate prosocial behaviors such as helping or being polite to others."[200] A similar study found that the use of "array microphones," i.e., distributed sound sensors that are hard to see, instead of a standard microphone had a profound effect on people's creativity and willingness to express themselves.[201]

As one set of experimenters opined:

> A general explanation for these results holds that the presence of others (whether real, implied, or imagined)

---

[195] *Id.*

[196] Woods *supra* note 13.

[197] *Id.*

[198] *Id.*

[199] Judson *supra* note 13 ("In the weeks with eyes, people paid more than they did in the weeks with flowers.").

[200] *Eye of the Camera* at 61.

[201] WIRED FOR SPEECH at 164. *See also id.* ("These findings should apply not just to array microphones but to any technology.").

> makes one a potential object of evaluation. Awareness of this fact directs attention to the self, that is, increases self-awareness and triggers self-evaluation ("what impression do a I make on others?") and impression management behavior, destined to ensure approval…[202]

In sum, any technology that suggests the presence of a person—the ability to manipulate symbols (i.e., language),[203] the appearance of voices,[204] eyes,[205] gestures and locomotion,[206] or the ability to transmit information to a remote party[207]—make us think that a person is really there. This in turn triggers a variety of reactions and behaviors associated with being in the presence of others, which vary with the degree of anthropomorphosis. Associated behaviors include cooperation, politeness, and affection, but also self-consciousness, self-promotion, and changes to what we are comfortable doing or disclosing.

C. Privacy

Much has been written, and much remains to be, about the underlying value of privacy. One recurrent theme in the literature, however, is that privacy helps create and safeguard moments when people can be alone. Hannah Arendt characterizes a "life spent entirely in public, in the presence of others" as "shallow."[208] Ruth Gavison speaks of the "terrible flatness" of a person who succeeds in giving up all privacy.[209] Barrington Moore sees privacy as "an escape from the demands and burdens of social interaction."[210] As Alan Westin famously wrote in his 1970 treatise, people require "moments 'off stage' when the individual can be 'himself'; tender, angry, irritable, lustful, or dream filled."[211] Privacy provides a "respite from the emotional stimulation of daily life."[212] "To be always 'on' would

---

[202] *Eye of the Camera* at 62.
[203] MacDorman & Ishiguro *supra* note 27.
[204] WIRED FOR SPEECH at 4.
[205] Wood *supra* note 13; Judson *supra* note 13.
[206] THE MEDIA EQUATION.
[207] *Eye of the Camera* at 62.
[208] HANNAH ARENDT, THE HUMAN CONDITION 71 (1958).
[209] Gavison *supra* note 54 at 443.
[210] BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 73 (1984) quoted in UNDERSTANDING PRIVACY at 75; *see also id.* at 163-64 (meticulously detailing the role of solitude in daily life).
[211] WESTIN *supra* note 17 at 35. The Supreme Court of India has also described privacy "a sanctuary [where] individuals can drop the mask." UNDERSTANDING PRIVACY at 164.
[212] WESTIN *supra* note 17 at 35.

destroy the human organism."[213]

A related role for privacy is to avoid interference with natural curiosity, introspection, and self-determination. Without privacy, the argument runs, we could become a nation of complete conformists. For Westin, privacy protects "minor non-compliance with social norms" that "society really expects many persons to break" in pursuit of truth and self.[214] Julie Cohen argues that "pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. … The condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it." [215] Gavison warns that even "casual observation has an inhibitive effect on most individuals that makes them feel more formal and uneasy."[216] Paul Schwartz has also written on the relationship of privacy to self-determination.[217]

"Some privacy problems create another kind of harm," notes Solove, in that "they inhibit people from engaging in certain activities."[218] The potential of excessive surveillance to curtail action, including free speech, is generally referred to as its "chilling effect."[219] The idea is that individuals under surveillance, with or without an accompanying threat of adverse action, will change their behavior in the individual instance, or refrain entirely from engaging in certain behavior for fear of retribution or judgment.[220] As Charles Fried notes in his *Anatomy of Values*:

---

[213] *Id.* Psychology also points toward the importance of solitude to maintaining good mental health. There is even some cross-species support for this notion, in that many animals prefer to perform certain functions in private. UNDERSTANDING PRIVACY at 163.

[214] WESTIN *supra* note 17 at 36.

[215] Julie Cohen, *Examined Lives: informational Privacy and Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000).

[216] Gavison *supra* note 54 at 447.

[217] Schwartz *supra* note 76; Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999). *See also* UNDERSTANDING PRIVACY at 94 ("Privacy enables people to escape from the relentless force of self judgment, which in too pervasive a dose can stunt self-development."). The absence of privacy is also a common feature of dystopian novels. *See, e.g.*, GEORGE ORWELL, 1984 (1949) (houses have two way video screens); YEVGENY ZAMYATEN, WE (1927) (buildings are transparent); ALDUS HUXLEY, BRAVE NEW WORLD (1932) (characters conditioned with a distaste for solitude).

[218] UNDERSTANDING PRIVACY at 178.

[219] *See, e.g., Laird v. Tatum*, 408 U.S. 1, 11 (1972) ("In recent years, this Court has found in a number of cases that constitutional violations may arise from the deterrent or 'chilling' effect of governmental regulations that falls short of direct prohibition against the exercise of First Amendment rights.").

[220] UNDERSTANDING PRIVACY at 108 ("Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her

> If we thought that our every word or deed were public, fear of disapproval or more tangible retaliation might keep us from doing or saying things which we would do or say if we could be sure of keeping them to ourselves.[221]

Technology as an independent medium implicates each of these privacy values.[222] It does so directly and measurably, and without necessarily collecting, processing, or disseminating any new information.

1. The mere presence of social machines in historically private places threatens solitude.

"The benefits of informational privacy are related to, but distinct from, those afforded by seclusion from visual monitoring," states a leading text book on information privacy.[223] "It is well-recognized that respite from visual scrutiny affords individuals an important measure of psychological repose. Within our society, at least, we are accustomed to physical spaces within which we can be unobserved."[224]

Machines, and particularly computers, go in many places historically reserved for solitude and reflection. "With the growth of embedded computers, computing applications are becoming commonplace in locations where human[s] would not be welcome, such as bathrooms or bedrooms, or where humans cannot go."[225] We carry increasingly sophisticated computers on our person, in our mobile phones, MP3 players, and other devices. We rely on computers to work, play, and connect. It is no exaggeration to say, with artificial intelligence expert H.R. Ekbia, that "[c]omputers are everywhere."[226]

As discussed above, robots too are entering the home, the car, and other

---

behavior.").

[221] CHARLES FRIED, AN ANATOMY OF VALUES 370 (1970).

[222] There are of course many more values that privacy helps protect. This Section deals with only two or three related values around solitude and chilling effects.

[223] DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW (3d ed 2009).

[224] *Id.*

[225] *See* P.J. Fogg, PERSUASIVE TECHNOLOGIES: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 10 (2003).

[226] Ekbia *supra* note 100. *See also* Jerry Kang and D. Cuff, *Pervassive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 94 (2005) ("[T]he Internet will soon invade real space as networked computing elements become embedded in physical objects and environments.").

spaces at an accelerating rate.[227] Whereas once robots were limited to the factory assembly line or surgical operation table, they are rapidly become a mainstream phenomenon. Costs are plummeting, and the market for personal robotics continues to expand.

Imagine a world, hardly implausible in light of the direction of design, where a technology that we are hardwired to accept as human occupies most private spaces. Robot toys and "butlers" wander the home. Voice-driven appliances and lights respond to commands. Cars interact with the driver—giving directions, warning of problems, or just chatting. Mobile phones interrupt with advice. Websites are hosted by avatars complete with personalities befitting the service. Searches for information feel like a conversation with a real person.

Meanwhile, we constantly feel the presence of another.[228] We live in a state of near constant psychological arousal.[229] We get even fewer "moments offstage," away from the "whirlwind of daily life."[230] We have more "free time," in the sense of fewer tasks to perform, but we are seldom completely free of the subconscious sense of judgment or evaluation. At the margins, this feeling of constant observation threatens to dampen creativity,[231] skew our thoughts and actions toward the mainstream,[232] and hinder self-development[233] in much the same way as actual ubiquitous surveillance.[234]

This privacy harm is particularly problematic in that it is often subconscious, subtle, and invited. It is not as though the government is placing computers or robots in our homes. We choose to adopt the underlying technology—in fact, we pay good money for it. Privacy law as presently formulated is ill-equipped to deal with unintentional, diffuse harm such as decreased internality and solitude.[235] First, notice and consent defeats most privacy cases. Second, the law is reticent to recognize

---

[227] *See supra*.
[228] *See supra*.
[229] *See supra*.
[230] WESTIN, *supra* note 17 at 35.
[231] WIRED FOR SPEECH at 159.
[232] Cohen, *supra* note 215 at 1425.
[233] Schwartz *supra* notes 76 and 217.
[234] *Cf.* Arthur Miller, *Privacy: Is There Any Left?*, 3 FED. CT. L.R. 87, 100 (2009) ("It does not matter if there really is a Big Brother on a screen watching us. It does not matter in the slightest. The only thing that matters is that people think there is a Big Brother watching them.").
[235] UNDERSTANDING PRIVACY.

subjective harms especially where, as here, the particular privacy harm is not long established.[236] Finally, because the phenomenon does not rely on the transfer of information, traditional privacy protections such as anonymization and encryption offer little help.

One might argue that humans will adjust to social machines and software the way the rich adjust to servants, the poor adjust to living on top of many relatives, or the chronically ill get accustomed to pharmacists, nurses, orderlies, and doctors. We may, after a time, feel solitude among machines as we acclimate to their presence.

This claim is not as reassuring as it might seem. What evidence there is suggests that the effects do not wear off.[237] Most social effects from technology occur irrespective of the individual's familiarity or comfort with the underlying technology.[238] It turns out, for instance, that "familiarity with interactive computers … removes neither the tendency nor the desire to interact with them as in a social context."[239]

Nor is it clear that people will come to trust computers and machines in quite the same way as, for instance, relatives and servants—assuming they do.[240] As Charles Fried aptly notes, "[o]ne does not trust machines or animals; one takes the fullest economically feasible precautions against their wrongs."[241] People are equally likely to treat robots like cameras or microphones, which seldom lend any greater appreciation of who is monitoring. At a minimum, research would be needed to conclude one way or another whether we will be able to recalibrate our notion of "alone" in light of evolving technology.

2. Introducing anthropomorphic design into communications transactions threatens to chill curiosity.

In a previous century, many of our communications were mediated by actual people. Telegraphers in the nineteenth century transmitted messages

---

[236] *See supra* Part I.

[237] For instance, the study in *Biology Letters* of payment on the honor system took place over 10-weeks, with no obvious lag in the effect. Melissa Batson *et al*., *Cues of Being Watched Enhance Cooperation in a Real-World Setting,* BIOLOGY LETTERS, 2(3):412–14 (2006) (noting similar effects at weeks one and nine).

[238] *See* THE MEDIA EQUATION at 252.

[239] Parise et al *supra* note 169 at 140.

[240] The claim that people were or remain comfortable around servants is largely anecdotal.

[241] FRIED *supra* note 221.

by hand across long distances. Early telephone customers shared common lines. To entice consumers concerned about privacy, advertisements appealed to class:

> Telephones are rented only to person of good breeding and refinement. … There is nothing to be feared from your conversation being overheard. Our subscribers are too well bred to listen to other people's business.[242]

Eventually, telephone calls become person to person through a dedicated line. "The central switchboard solved the immediate early problem of having to connect with every other telephone," explains Irving Fang in *A History of Mass Communication*, "but the central switchboard required telephone operators who were not always attentive and might listen in."[243] Accordingly, operators were screened from the ranks of polite and upstanding young women. As David Mercer relates: "One of Bell's first female switchboard operators, Katherine Schmitt, suggested that the operator 'must be a paragon of perfection, a kind of human machine.'"[244]

Today (non-human) machines mediate most of our communications. This resolves the issue of an intermediary "listening in," at least in the ordinary case.[245] As Richard Clarke and many others point out, however, this mediation leads to a distinct set of privacy concerns.[246] Computers can record every call and keystroke.[247] Internet advertisers track users as they surf from site to site across a network. Search engines record a log of queries, pairing the text of the search with a unique identifier and other information.[248] Meanwhile, all of this information can be linked and searched. It is in fact this increased capacity to collect, process, and disseminate that informs most privacy and technology scholarship.

But modern computer users don't necessarily *feel* as though they are being tracked. We may know, as an intellectual matter, that somewhere, someone might eventually pick up our digital trial. But the experience of searching, surfing, or emailing is actually a lonely one. We're aware of no

---

[242] IRVING FANG, A HISTORY OF MASS COMMUNICATION 86 (1997).

[243] *Id.*

[244] DAVID MERCER, THE TELEPHONE: THE LIFE STORY OF A TECHNOLOGY 52 (2006).

[245] Clearly the government and private snoops can still listen in under certain circumstances.

[246] Richard Clarke, *Information Technology & Dataveillance*, *in* CONTROVERSIES IN COMPUTING (C. Dunlop, R. Kling eds 1991).

[247] *See* O. Kerr *supra* note 29 at *7; O. Kerr *supra* note 92 at 565.

[248] Omer *supra* note 2.

operator lurking on the line. In the moment, we don't expect anyone other than our intended recipient to read our email. We don't expect any company employee, hacker, or government official to link our searches with us, personally. Modern communication overwhelmingly feels anonymous, even when it isn't.[249]

The subjective experience of "having company" entails serious repercussions for attitude, comfort, and behavior. Reminders of the possibility of observation, or even the remote presence of another human, alters what and how we communicate and perform tasks. The presence of visible microphones, for instance, inhibits creativity and self-disclosure. The same is true of cameras, even where the subjects are told that the cameras are off.[250]

As discussed in the preceding section, we have begun to reintroduce the functional equivalent of humans into our communications transactions. Search is the gateway to most Internet experience. Its largest provider is moving in the direction of voice and natural language, both of which act as strong anthropomorphic signifiers likely to provoke significant user reactions. Today individuals search alone. We type text into a box and get text results. Tomorrow's searches will feel a discussion between the user and an autonomous expert.[251]

This in turn has implications for privacy. Specifically, it threatens an immediate and visceral chilling effect on our information transactions. Introducing an apparent agent into the "media equation" can measurably alter self-presentation and modulate disclosure. Changes to interface technology will suddenly present us with a partner as we explore and transact. Searching for controversial content, checking embarrassing symptoms, exploring fringe ideologies, criticizing our institutions, and finding information about homosexuality will occur through what we are hardwired to feel is a personal. Meanwhile, no amount of encryption or anonymization (i.e., removing personally identifiable information) will lessen the harm because, again, information is not the issue.

---

[249] *Enter Search Term Here, Forever*, N.Y. TIMES, Aug. 21, 2006 ("When people search the Internet in their homes, it feels like a private activity.").

[250] *Eye of the Camera*.

[251] *See* BATTELLE *supra* note 20 ("As we learn new ways to interact with information, it will stop looking like a list of links and will start feeling more like a conversation.").

3. Our reactions to social design also creates opportunities for better online privacy notice.

Thus far this Part has revealed a hidden dimension to privacy and discussed its potential downsides. But the ability of technology to create the sensation of being observed also presents a novel opportunity to enhance privacy. Specifically, placing an apparent agent at the site of data collection can help line up user expectations about how data will be used with the actual practices of the entity collecting that data. A form of "visceral notice"—in the sense that the technique directly conveys the reality that user information is being collected, used, and often shared—could help shore up a failing regime of textual notice.

A common complaint among privacy commentators is that users are not aware of the extent to which companies and others collect, share, and use their data, particularly on the Internet.[252] Governments have in cases intervened, generally requiring that the company disclose its practices in writing. For instance, a California law requires "commercial website operators" who collect personally identifiable information to write a privacy policy and place a "conspicuous" link to it everywhere they collect such data.[253] Among other things, the policy must state what categories of information the website collects, the uses to which it puts that information, and the third parties with whom the information might be shared.[254]

The trouble is that few people read privacy policies.[255] Worse yet, many people think that the mere existence of a privacy policy means that companies cannot use or share data in particular ways.[256] Internet companies also face incentives to word their policies as broadly as possible so as to facilitate future innovative uses of consumer data and avoid liability.[257]

---

[252] *See, e.g.*, Dan Solove, *Privacy & Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393 (2001). *See also* Daniel Solove, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 6-9 (2004); Froomkin *supra* note 53; Omer *supra* note 2.

[253] California Online Privacy Protection Act, BUS. & PROF. CODE §§ 22575-22579 (2004).

[254] *Id.*

[255] Fred Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF INFORMATION 361 (2006). According to one report, only .03% of the users read clicked on a website's privacy policy. *Id.*

[256] *See* Chris Jay Hoofnagle & Jennifer King, *Research Report: What Californians Understand About Privacy* SSRN eLibrary (2008).

[257] Google is always looking for new ways to organize and present data, including user data. Its privacy policy is correspondingly broad in scope, stating that Google can

Human-computer interfaces that introduce an apparent person at the site of collection may resolve the notice problem in a direct and more salient way: through a visceral reminder that the data being collected will be used and shared. Changing from an array microphone to a standard one, for instance, changes what people disclose.[258] So does the introduction of a camera and/or a warning sign.[259] Online, the use of such techniques short-circuits the need to read lengthy and broadly worded policies and cuts off the concern that the words "privacy policy" will imply responsible practice. The overuse of anthropomorphic design might chill curiosity and interrupt internality, but the use of properly calibrated social interfaces to collect sensitive data could help line up privacy expectations with information experience.

Best practices suggest that companies should not store or share data in the first place beyond what is necessary to accomplish the service.[260] But where they do collect and use data, a hard-wired reminder not to share intimate details could be a useful tool to improve upon the sorry state of notice. Paradoxically, the use of visceral notice may also have the effect of improving user trust; research shows that, in addition to placing users on alert, anthropomorphic design actually increases user trust in the website.[261]

III. APPLICATION

This Article has largely focused on ways of thinking. Part I presented the dominant conception of technology's relationship to privacy as instrumental and focused on the manipulation of data. Part II supplemented that conception by introducing a new frontier—interface experience—complete with additional privacy dangers and opportunities. This Part begins to apply the preceding insights to real problems in scholarship,

---

"combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. Google Privacy Policy, *at* http://www.google.com/privacypolicy.html (last visited April 28, 2009); *see also* Yahoo! Privacy Policy, *at* http://info.yahoo.com/privacy/us/yahoo/details.html (last visited April 28, 2009) ("Yahoo! uses information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.").

[258] *See* WIRED FOR SPEECH at 159.

[259] *See Eye of the Camera*.

[260] *See, e.g.*, Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, Feb. 2009, 46-47.

[261] *See supra* note 193 and accompanying text.

regulation, and policy. It is meant to be illustrative, not exhaustive.

Section A begins by analyzing two existing technologies (voice-driven search and personal robotics) from the traditional privacy perspective of data manipulation. The section then demonstrates the value of a further analysis of interface design based on user experience. Section B seeks to inform regulation by looking at both aspects of the misalignment of experience and actual practice. This Section explores warning consumers where a service or device might have a negative but initially imperceptible impact on their experience and behavior. It also recommends caution against the excessive use of technology that creates the perception of observation, particularly by the government.

A. Analysis

1. Voice-driven search.

As discussed in detail above, mobile Internet search has already moved in the direction of voice. Users may search for items by speaking the query into the phone rather than typing it into a text box. This frees up users to search on the go, even while driving a car. Voice recognition has come far enough that almost all queries are recognized instantaneously.

It is clear that this technology implicates privacy in some way. As with all search engines, users must send potentially sensitive information to a remote company in order to get back results. In addition to the search queries themselves, search engines typically collect and maintain a log of when the search was made, the Internet Protocol ("IP") address from which it derived, and other information.[262] Companies can also process data across multiple searches in an effort to improve their services and advertising.

Under certain circumstances, search queries and associated data can be disclosed to third parties. Internet companies may share such data among affiliates. Prosecutors or private litigants may subpoena the data—in an aggregate or individual form—for a variety of reasons. The information may even be released involuntarily due to a security vulnerability.[263] Finally, users themselves may use search engines to invade one another's

[262] *See generally* Omer *supra* note 2.

[263] In a well publicized event, AOL purposefully released use research terms for research purposes, some of which were linked back to individuals.

privacy through "search-stalking."[264]

Traditional privacy analysis captures each of these dimensions. It may also recognize specific harms related to the fact that the search query is spoken out loud instead of typed. Voice adds important layers to the data that is collected, which in turn permits novel harms. Specifically, voices are unique and self-identifying.[265] Unlike most test queries, voice data could be used to assess the individual's state of mind at the time of search—did they sound angry, drunk, or sad?—or demographic information such as their gender, age, and race.[266]

Traditional analysis, grounded as it is in an instrumentalist view of technology, probably ends here. Yet voice-search implicates privacy in other ways, involving the way the user *experiences* the technology. In addition to sending information, for instance, voice search may limit what users feel safe surfing for in ways related to how the experience of speaking differs from the experience of writing. Unless the user is out of earshot, he or she may not want to search for local strip clubs or the proper treatment of you-name-it disease. Even a user who is alone may refrain from certain searches out of discomfort at giving voice to a controversial or objectionable fantasy or desire.[267]

More basically still, because of the "automatic and powerful responses elicited by all voices, whether human or machine in origin,"[268] the mere existence of a voice prompt may trigger a state of psychological arousal. The user of voice-based search may relax as though alone, with measurable effects to her attitudes and behavior. This travelling, routine reminder that a person is present may interrupt possibilities for solitude and exert a subtle chill on the user's curiosity—to the same or greater degree as any technology designed to observe.

---

[264] *See* Surden *supra* note 62.

[265] *Cf.* ENGAGING PRIVACY at 22 (noting that "the biometric of voice recognition can be used as an identification mechanism for vocal forms of communication").

[266] As just one example of a use case: imagine that a fresh wave of terrorist attacks by foreign fundamentalists prompts the Transportation Security Administration to (1) require an Internet search engine with a voice interface to flag any instance of an accented person requesting information about explosives, and (2) use the information as a data point in compiling its "No Fly List."

[267] As an experiment, try typing the words "hardcore pornography" and then saying the words "I am looking for some hardcore pornography" aloud.

[268] WIRED FOR SPEECH at 4.

2. Intel's Home Exploring Robotic Butler.

Herb is semi-autonomous robot under development by Intel. Herb is capable of mapping out a house through unassisted exploration and performing a number of tasks in response to verbal instructions.[269] According to its team of inventors, Herb is designed to improve on current personal robots—such as Roomba—that only provide task-specific functions and suffer from being "unanthropomorphic" (in the sense of not being well adapted to a human home). Herb seeks to add to the range of home tasks that "assistive agents" are capable of performing.[270]

Does Herb implicate privacy? A traditional analysis will again begin with the sorts of information that Herb—or Intel—collects, processes, and discloses. There is a well-understood difference, for instance, between fleeting events and events that are recorded and stored.[271] Thus, were Herb to record data, his presence in the home may implicate privacy. Herb or, more likely, future Herbs, may also be capable of sensing events in the home that ordinary humans cannot such as electromagnetic forces or even changes in brain waves.[272] This too changes the privacy dynamic.

A different and arguably more serious privacy concern arises if Herb is networked in some way and periodically relays information to Intel or elsewhere. Privacy and criminal process laws typically regard the home as sacrosanct, requiring consent or a warrant before entry or internal surveillance.[273] If, however, the government can access Herb's sensor feeds in real time or from remote storage, then his introduction into the home may threaten longstanding protections. [274] Moreover, at least one study has shown vulnerabilities in robotic systems that could lead to privacy problems.[275]

---

[269] *HERB* at *2.

[270] *Id.*

[271] *See supra* Part I.

[272] *Cf. A Roadmap of U.S. Robotics: From Internet to Robotics*, CCC & CRA White Paper *76 ("Human-robot interfaces include … neural interfaces including physical probes, EEG (brainwaves), and surface EMG…"). On file with author.

[273] *See* U.S. CONST. AMEND. IV. *See also* UNDERSTANDING PRIVACY at __ (noting the historical importance of the home in privacy law).

[274] *See also Smith v. Maryland*, 442 U.S. 735 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). The notion that entrusting records to others lowers constitutional protection is known as the "third party doctrine." *See* SOLOVE & SCHWARTZ supra note __ at 333.

[275] *See* Tamara Denning *et al*, *A Spotlight on Security and Privacy Risks With Future Household Robots*, ACM (Sept.–Oct. 2009), on file with author.

These are important questions, but they do not present the entire picture. Our assessment of Herb's impact on the home must the experiences of the occupants. Even if Herb does not collect, process, or relay information in an excessive or irresponsible way, his mere presence has the potential to interrupt solitude and create the subjective feeling of being observed and evaluated.

In its current incarnation, Herb does not have a recognizable face. Herb is more akin to a robotic arm fashioned to a mobile platform.[276] This is not to say, however, that Herb lacks anthropomorphic features. The robot's ability to understand verbal commands, recognize objects, open doors, move with intention, and gesticulate may all occasion social responses from people.[277]

The question, which is an empirical one, is whether Herb's appearance and actions interrupts the solitude of household members or otherwise triggers social inhibition or discomfort. It might be that members of the household adjust to Herb's presence like that of a pet or a new member of the family. On the other hand, Herb may exist in a twilight between family and stranger—not unknown, but never fully known, like some permanent house guest.[278] These questions need to be asked and answered in a thorough privacy analysis.

B. Regulation

On the view this Article has developed, privacy harm is largely a function of the misalignment of expectation and actual practice.[279] Traditional misalignment occurs where information gets collected, processed, or disseminated to a greater extent than the data subject understands. But misalignment is also relevant to the extent the data subject

---

[276] *Id.*

[277] *See supra* notes __ - __ and accompanying text.

[278] As discussed in Part II.C.3, if Herb does in fact collect data and share data, it may be better for Herb to take on additional anthropomorphic features sufficient to align the robot's role as a data collector with the expectations it elicits. The more data a robot collects, the more anthropomorphic should its design be.

[279] By "actual practice," I do not mean the fact of monitoring but rather its outcome. One can imagine a society that is zealously monitored and knows it. Whether this society is worse off than a society that does not realize it is under observation depends on a variety of factors, including whether observation is invited or imposed top-down, who has access to the information it generates, and how that information is used. It may be that knowledge of observation compounds or even creates a privacy harm in certain circumstances. Where information will be used against a data subject, however, the harm is generally mitigated by knowledge, presenting the individual with the chance to protest or avoid the consequences.

experiences a perception of observation that is excessive or unnecessary, especially in spaces or transactions historically experienced as private. This means that new regulation may be necessary to capture technology's full range of impact on privacy. What this regulation might be is not clear and the purpose of this Article is primarily to identify the gap. What follows, however, are some initial possibilities.

If a commercial technology actually triggers non-obvious discomfort and social inhibition, there is an argument that consumers should be warned. As with any hidden danger, from carcinogens to subliminal advertising, harmful reactions to social technology of the sort explored in Part II are not obvious and hence cannot be avoided through notice and choice.[280] With some exceptions, we understand when we are talking to a person rather than to a device. We adopt the technology voluntarily because we find it attractive or otherwise convenient. But the literature is clear that our brains react to the technology at a deeper, unperceived level. It may be worth warning consumers of personal robotics, therefore, that the presence of the robot may have the same impact—on physiology, task performance, relaxation, etc.—as the presence of a person.[281]

We should in general be very wary of the use of technologies that purposively make citizens feel observed. It is today routine for transportation authorities to introduce pictures of faces and eyes, along with a request to assist law enforcement by reporting anything suspicious, in an effort to combat crime.[282] As previously discussed, the U.S. government is well-acquainted with the ability of technology to substitute for people.[283] The government is today funding efforts to improve such technology, just as it funded voice-recognition labs in the 1970s.[284]

Will our hardwired reactions to social design be used as a behavior disincentive? In what contexts and to what extent? Given the dangers, we should apply our traditional First Amendment skepticism of excessive "chilling effects" to new technologies that leverage our hardwired reaction

---

[280] *See In re Int'l Harvester Co.*, 104 F.T.C. 1070 (1984) (discussing the elements of unfairness as a substantial injury that cannot be reasonably avoided and is not outweighed by offsetting benefits).

[281] We could also require that robots come with a cover, or that companies offer an alternative to voice and character interaction. And of course the opposite is true; we can require websites, robots, or other technologies that collect information to reflect a proportionate degree of anthropomorphic design.

[282] *See* Judson *supra* note 13.

[283] *See supra* notes __ to __ and accompanying text.

[284] *See supra* notes __ to __ and accompanying text.

to social design. The purposive exploitation of our natural propensity to behave in the presence of others, coupled with our inability to distinguish between real or virtual surveillance, could substitute for direct prohibitions on speech or investigation.[285]

Again, these are just two of many ideas. The first step is recognition by privacy scholars, designers, and eventually consumers and regulators of the underlying phenomenon.

CONCLUSION

There's an old Victor phonograph commercial featuring a dog showing a great deal of interest in a cone-shaped speaker. The caption reads "His master's voice" and the idea is that the dog cannot differentiate between the illusion and the real deal.[286]

It turns out that we're a little like the dog in the ad. At some basic, hardwired level, we have trouble differentiating between real voices, conversations, and faces and technology that imitates them. And because of this, we unwittingly adopt technologies with the potential to interrupt solitude and chill speech without need, in the sense that no information is actually being used against us. This harm is all the more dangerous in that it is subconscious, voluntary, and cannot be remedied with traditional privacy safeguards.

In looking too narrowly at technology's impact on privacy, we may also be missing a serious opportunity to improve the failing regime of notice. Rather than merely representing textual information in an incrementally easier format, we should think about leveraging our hardwired reaction to technology in order truly to line up expectations with actual information practice. We should not invite unnecessary feelings of observation, but we should consider creating those feelings where there really is a danger that our data will be used and collected in ways that affect us. We're also missing classic venues where consumer protection laws or limits on government are commonly though appropriate.

This Article opens the door onto a new frontier of privacy and

---

[285] *Cf.* Arthur Miller, *Privacy: Is There Any Left?*, 3 FED. CT. L.R. 87, 100 (2009) ("It does not matter if there really is a Big Brother on a screen watching us. It does not matter in the slightest. The only thing that matters is that people think there is a Big Brother watching them.").

[286] For a picture and discussion of the ad, visit http://www.victor-victrola.com/.

technology scholarship in and beyond the law. Communications scholars should think explicitly about "computers as social actors" theory and other experiments involving the substitution of technology for people as implicating solitude and free speech. Privacy scholars, meanwhile, should think beyond the collection, processing, and dissemination of information when assessing the impact of technology. Finally, regulators and industry should recognize the dangers and opportunities for privacy inherent in our visceral reactions to anthropomorphic design.