

Dredging-up the Past: Lifelogging, Memory and Surveillance

Anita L. Allen

What if I stored everything, what would it mean, what are the implications? We don't know." – Jim Gemmell¹

An exhibit at the 1939 New York World's Fair popularized the idea of preserving a comprehensive depiction of human life in a compact medium of storage. The Westinghouse Corporation stuffed a remembrance of America into a glass container sealed inside an 800 pound, bullet-shaped canister made of copper, chromium and silver.² Today, we use the term "time capsule" to describe just about anything intended to preserve the past for the future. The original, Westinghouse time capsule housed specific articles selected by a committee formed to design an optimal record of national life for retrieval in five millennia. The Westinghouse Committee stocked its time capsule with small commonly used articles, textiles and materials, and miscellany including books, money, seeds, and scientific and electrical devices. The Committee also elected to store documents on microfilm, a newsreel of current events, and messages from Albert Einstein and other "noted men of our time". In case the world forgets, a time capsule affords a means to remember.

1 Alec Wilkinson, Remember This? A Project to Record Everything We Do In Life, The New Yorker, May 28, 2007, pp. 38-44.

2 A New York Times sponsored web page lists the complete contents of the Westinghouse time capsule. See <http://www.nyt.co..specials/magazine3/items.html>.

In 1974, the artist Andy Warhol began what was described as a “time capsule” project of his own,³ a query of his generation’s notions of transience, permanence, and history. Warhol’s medium of storage was ordinary cardboard boxes. Rather than attempting to fill the boxes with artifacts of collective importance, Warhol preserved random items that accumulated on and around his own desktop.⁴ When a particular box was full, Warhol closed, dated and stored it. Warhol’s died in 1987, leaving for the future a solipsistic collection of personal clutter. The Andy Warhol Museum in Pittsburgh, Pennsylvania houses 610 of the artist’s cardboard boxes, preserving details of his unique life and frenetic social milieu. Ironically, because Warhol evolved from celebrity artist to cultural icon, his campy, fragile, self-involved time capsules preserved collective remembrance after all. Long into the future, trash or treasure, his boxes are being inventoried, catalogued, photographed, studied and conserved in light, humidity, temperature and access-controlled rooms.

3 For a description of Andy Warhol’s time capsule project, see <http://www.warhol.org/collections/archives.html> (“This serial work, spanning a thirty-year period from the early 1960s to the late 1980s, consists of 610 standard sized cardboard boxes, which Warhol, beginning in 1974, filled, sealed and sent to storage. . . . Photographs, newspapers and magazines, fan letters, business and personal correspondence, art work, source images for art-work, books, exhibition catalogues, and telephone messages, along with objects and countless examples of ephemera, such as announcements for poetry readings and dinner invitations, were placed on an almost daily basis into a box kept conveniently next to his desk.”)

4 See id. See also, [Robin Pogrebin](#), A Portrait of an Artist Both Loved and Hated, New York Times, September 20, 2006.

Andy Warhol deliberately wove archiving into the fabric of his everyday life for years, allowing the happenstance of solitary and social experience substantially to dictate the items he saved. Warhol thus represents a drift in emphasis from ceremonial, episodic preservation of the memory of a whole, imminent society (illustrated by the Westinghouse time capsule), to informal, continuous preservation of the memory of a single, singular individual. Andy Warhol's art project has significance for another reason. It bridges the gap between the quasi-scientific futurism of 20th century time-capsuling and the technological conceit of 21st century "lifelogging".

A. Lifelogging

The term "lifelog" refers to a comprehensive archive of an individual's quotidian existence, created with the help of pervasive computing technologies: "A lifelog is conceived as a form of pervasive computing consisting of a unified digital record of the totality of an individual's experiences, captured multimodally through digital sensors and stored permanently as a personal multimedia archive.⁵ Lifelog technologies would record and store everyday conversations, actions, and experiences of their users, enabling future

⁵ See Martin Dodge and Rob Kitchin, 'Outlines of a World Coming into Existence': Pervasive Computing and the Ethics of Forgetting, 34 *Environment and Planning B: Planning and Design* 431-445 (2007), emphasis in the original. See also Martin Dodge and Rob Kitchin, *The Ethics of Forgetting in an Age of Pervasive Computing*, CASA Working Paper Series, www.casa.ucl.ac.uk, http://www.casa.ucl.ac.uk/working_papers/paper92.pdf, characterizing lifelogs, inter alia, as "sociospatial archives that document every action, every event, every conversation, and every material expression of an individual's life."

replay and aiding remembrance. The emergent interest in the concept of lifelogging stems from the growing capacity to store and retrieve traces of one's life via computing devices. Products to assist lifelogging are already on the market;⁶ but the technology that will enable people fully and continuously to document their entire lives is still in the research and development phase.⁷ Creative inventors like Steve Mann have led the way.⁸

“MyLifeBits” is the name of a Microsoft Research company-sponsored full-life lifelogging project conceived in 1998 to explore the potential of digitally chronicling a person's life.⁹ MyLifeBits focuses on preserving the life of veteran researcher Gordon Bell.¹⁰ MyLifeBits is high concept, high tech, labor intensive, and Warhol-like: continuous storage of a life in durable electronics rather than paper cartons.¹¹ Using an

6 Full-life, lifelog recordation is a thing of the future. However, lifelog products are already on the market. A Nokia product, Lifeblog, archives cell phone messages and photographs, see <http://www.geekzone.co.nz/content.asp?contentid=2466>. Weblog technology that enables users to record thoughts, photos, video and audio are being marketed under the “lifelog” rubric. See <http://www.reallifelog.com/>.

7 See generally, Martin Dodge and Rob Kitchin, *Outlines of a World Coming*, supra, note —.

8 University of Toronto professor Steve Mann has been a pioneer in the field of wearable computers, counter-surveillance and lifelogging. See <http://wearcam.org/steve.html>. and <http://www.eyetap.org/>. See also http://www.eyetap.org/papers/docs/ieee_media.pdf, comparing Mann's “Eye Tap” lifelogger, which alters the image of the world presented to the logger, to MyLifeBits.

9 See supra, note 1, quoting Gemmell. See also Gordon Bell and Jim Gemmell, *A Digital Life*, 296 *Scientific American* pp. 58-65 (March 2007).

10 Id. Gordon Bell and Jim Gemmell, *A Digital Life*, 296 *Scientific American* pp. 58-65 (March 2007).

11 Electronic media of storage raise problems of transience. Bell recognizes that parts of his archive could become unreadable one day. If the technology of “jpeg” were

infrared “Sensecam” camera worn around his neck, scanners, and computing devices, Mr. Bell records nearly all of his conversations and experiences. He stores them electronically, along with documents, photographs and memorabilia chronicling his past. In addition, Mr. Bell electronically preserves all of his email, typed documents, and web pages visits. Although Mr. Bell makes use of a human assistant and an ad hoc array of clunky wearable and desktop devices requiring self-conscious acts of collection and storage, technologists imagine a future of automatic, customizable, continuous and virtually “invisible” lifeloggers. Lifelogging devices will be inexpensive in the future, too. Mr. Bell estimates that 60 years of human experience constitutes one terabyte of data. That amount of data can be stored on a \$600 hard drive today, but tomorrow will be storable on cheap cell phones, as cheap as Andy Warhol’s cardboard boxes.¹²

Biological memory serves us well, but it is highly selective and fallible.¹³ We do not remember all of our conscious experiences; we misremember many of our experiences; and memory fades over time.¹⁴ Even what is objectively memorable can be

supplanted, for example, stored images would become inaccessible. See supra note __ at 44 (“A lot of things you may not be able to read a decade later... . Will the jpeg format still be in existence? Will Microsoft 6 be readable?”)

12 Clive Thompson, *A Head for Detail*, *Fast Company* 73-78 and 110-112, at 77 (2006) (describing Gordon Bell and other experimental innovators who are feeding the details of their lives into “a surrogate brain”).

13 Daniel L. Schacter, *The Seven Sins of Memory: How the Mind Forgets and Remembers* (2001).

14 Cf. H. Branch Coslett, *Consciousness and Attention*, 17 *Seminars in Neurology* 137 (1997) (memory and brain disorder researcher describing the relationship between attention and consciousness).

forgotten. Stricken with Alzheimer disease, Ronald Reagan forgot he had been President of the United States. To address the problem of fallible memory, the ancients relied on mnemotechnology, story-telling, pictures, and, eventually uniform systems of writing.¹⁵ Lifelog innovators are promising to better the ancients with their memory machines. The idea of a memory machine was once pure fantasy.¹⁶ But technologists predict that full-life, lifelogging devices will one day be integrated into everyday existence, becoming as ordinary as telephones.¹⁷ Ancillaries to memory, lifelogs will enable unprecedented accurate retention and recall of personal life. By design, lifelogs could be substantially less selective and less fallible than human memories stored only in the brain.

Envisioning a less fallible and selective adjunct to human memory, Total Recall is a lifelog research project of the Internet Multimedia Lab of the University of California.¹⁸

15 Cf. Frances A Yates, *The Art of Memory* (1966) (ancient Greek and Roman developed a “mnemotechnology” of improving the ability to remember details of argument and perspective by associating ideas with visual, often architectural imagery.)

16 See Jose Van Dijck, *From Shoe Box to Performative Agent: The Computer as a Personal Memory Machine*, *New Media and Society*, Vol 7 (3) 311-332, 314-316 (2005), describing the “Memex” machine fantasy introduced in Vannevar Bush’s July 1945 *Atlantic Monthly* article, “As we May Think.”

17 See generally, *id.*, at 319-324, describing *Lifestreams*, *Memories for Life* and *MyLifeBits* visionary life-log projects, all aimed preserving life experiences in a seamless, invisible way that exploits digital technologies.

18 For a description of the Total Recall project at the University of Southern California, see <http://bourbon.usc.edu/iml/recall/> (“The aim for the Total Recall project is to design and develop a personal information management system which will securely collect, store, and disseminate data from a variety of personal sensors. It will also allow customizable searching, analysis, and querying of this data, in a secure manner. Numerous applications of such systems will play an important role in improving people's

Total Recall researchers maintain that technologies to “amass memories, experiences, and ultimately knowledge from an individual perspective” through the use of personal sensors and recording devices will “likely change social structure”.¹⁹ They anticipate mostly positive changes and net benefits relating to education, law enforcement, health care, and sense and memory enhancement for the disabled.²⁰

The Defense Advanced Research Projects Agency (DARPA) is the central research and development arm of the United States Department of Defense.²¹ In 2003, DARPA solicited proposals for a LifeLog technology project with possible military applications. The lifelog technology DARPA conceived “can be used as a stand-alone system to serve as a powerful automated multimedia diary and scrapbook.”²² Moreover, “[b]y using a search engine interface,” the user of the lifelog DARPA hoped to create, could “easily retrieve a specific thread of past transactions, or recall an experience from a few seconds ago or from many years earlier in as much detail as is desired, including

quality of life.”). See also William Cheng, Leana Golubchik and David Kay, Total Recall: Are Privacy Changes Inevitable? CARPE October 15, 2004, p. 1.

19 See also Clive Thompson, A Head for Detail, Fast Company 2006 (describing Gordon Bell and other technologists and artists who are feeding the details of their lives into “a surrogate brain.”

20 William Cheng, Leana Golubchik and David Kay, Total Recall: Are Privacy Changes Inevitable? CARPE October 15, 2004, p. 1.

21 See for a general description of its mission, see DARPA’s website, <http://www.darpa.mil/>

22 See DARPA lifelog project solicitation, http://www.darpa.mil/ipto/solicitations/closed/03-30_PIP.htm

imagery, audio, or video replay of the event.”²³ Project LifeLog was short-lived; but during its evocative span, it invited the public to imagine the greater effectiveness of military commanders equipped with lifelogs and with access to lifelog data concerning the experiences of their troops.²⁴

For generals, edgy artists and sentimental grandmothers alike, lifelogging could someday replace or complement, existing memory preservation practices. Like a traditional diary, journal or day-book, the lifelog could preserve subjectively noteworthy facts and impressions. Like an old-fashioned photo album, scrapbook or home video, it could retain images of childhood, loved-ones and travels. Like a cardboard box time capsule or filing cabinet it could store correspondence and documents. Like personal computing software, it could record communications data, keystrokes and internet trails. The lifelog could easily store data pertaining to purely biological states derived from continuous self-monitoring of, for example, heart rate, respiration, blood sugar, blood pressure and arousal.

23 Id.

24 The federal government Defense Advanced Research Projects Agency (DARPA) abandoned its LifeLog project. In 2003 DARPA solicited proposals to develop LifeLog technology: “The objective of this "LifeLog" concept is to be able to trace the "threads" of an individual's life in terms of events, states, and relationships. . . . LifeLog can be used as a stand-alone system to serve as a powerful automated multimedia diary and scrapbook. By using a search engine interface, the user can easily retrieve a specific thread of past transactions, or recall an experience from a few seconds ago or from many years earlier in as much detail as is desired, including imagery, audio, or video replay of the event.” See http://www.darpa.mil/ipto/solicitations/closed/03-30_PIP.htm The Lifelog Project was not related to the controversial Terrorism (originally Total) Information Awareness, which was a scheme to use data-mining to piece together profiles of individuals. See generally, http://www.darpa.mil/ipto/solicitations/closed/03-30_PIP.htm

B. The Appeal of the Life Log

Is informal, continuous preservation of individuals' experiences using durable electronics a good thing? What is the value of creating an ultra-detailed electronic record of one's own existence? Why would anyone want to make a multimedia record of her entire life? The answer may be that our experiences and achievements comprise our uniqueness; preserving a record of them preserves a record of us. Lifelogging feeds the inner King Tut—the side of us that rejects transience through mummification, relic and entombment. But lifelogging is also journaling, art, entertainment and communication. Innovators expect lifelogging products to emerge as serious tools for improving the quality of life. In its favor, lifelogging might encourage introspection and self-knowledge. The capacity to share lifelogs could increase intimacy, understanding and accountability in personal relationships. Inheriting the lifelog of a deceased parent, spouse or child could help preserve family history and ease the pain of loss. Replay and remembrance machines could make us better at caretaking, work and professional responsibility, too. Finally, lifelogs might enhance personal security. A potential mugger or rapist would have to think twice in a society of lifeloggers.

To the extent that it preserves personal experience for voluntary private consumption, electronic lifelogging looks innocent enough, as innocent as Blackberries, home movies, and snapshots in silver picture frames. But lifelogging could fuel excessive self-absorption, since users would be engaged in making multimedia presentations about

themselves all the time. The availability of lifelogging technology might lead individuals to overvalue the otherwise transient details of their lives. With all due respect to Pico Della Mirandola's²⁵ majestic humanism and Immanuel Kant's²⁶ enlightened liberalism, most of every human life is as fungible and forgettable as a mass-produced soup can.²⁷ Furthermore, the potential would be great for incivility, emotional blackmail,

25 Pico Della Mirandola, *Oration in the Dignity of Man* (1486) (" I have figured out why man is the most fortunate of all creatures and as a result worthy of the highest admiration and earning his rank on the chain of being, a rank to be envied not merely by the beasts but by the stars themselves and by the spiritual natures beyond and above this world. This miracle goes past faith and wonder. And why not? It is for this reason that man is rightfully named a magnificent miracle and a wondrous creation. ... Finally, the Great Artisan mandated that this creature who would receive nothing proper to himself shall have joint possession of whatever nature had been given to any other creature. He made man a creature of indeterminate and indifferent nature, and, placing him in the middle of the world, said to him "Adam, we give you no fixed place to live, no form that is peculiar to you, nor any function that is yours alone. According to your desires and judgement, you will have and possess whatever place to live, whatever form, and whatever functions you yourself choose. All other things have a limited and fixed nature prescribed and bounded by Our laws. You, with no limit or no bound, may choose for yourself the limits and bounds of your nature. We have placed you at the world's center so that you may survey everything else in the world. We have made you neither of heavenly nor of earthly stuff, neither mortal nor immortal, so that with free choice and dignity, you may fashion yourself into whatever form you choose. To you is granted the power of degrading yourself into the lower forms of life, the beasts, and to you is granted the power, contained in your intellect and judgement, to be reborn into the higher forms, the divine." ... Imagine! The great generosity of God! The happiness of man! To man it is allowed to be whatever he chooses to be!" See <http://www.wsu.edu/~dee/REN/PICO.HTM>. See also <http://history.hanover.edu/early/pico.html>.

26 Immanuel Kant, *An Answer to the Question: What is Enlightenment* (1784) (" Enlightenment is man's emergence from his self-imposed immaturity. Immaturity is the inability to use one's understanding without guidance from another. This immaturity is self-imposed when its cause lies not in lack of understanding, but in lack of resolve and courage to use it without guidance from another. Sapere Aude! [dare to know] "Have courage to use your own understanding!"--that is the motto of enlightenment.""). See <http://www.english.upenn.edu/~mgamer/Etexts/kant.html>.

27 I allude, of course, to Andy Warhol's famous canvases depicting Campbell-brand soup cans, which render a mundane generic object, into something of interest. See generally http://edu.warhol.org/aract_soup.html.

exploitation, prosecution and social control surrounding lifelog creation, content and accessibility. This parry of the costs and benefits commences a fuller discussion of lifelogging's implications.

C. General Questions

The concept of lifelogging engenders numerous questions. What would it mean for society if typical individuals retained a detailed record of their entire lives? In a world of lifelogs, what would happen to beneficial forgetting, breaking with the past, and moving on? What would it mean for interpersonal relationships to know that shared experiences are probably being recorded? How will intimacy, confidentiality and privacy be affected? Question of freedom and compulsion arise. Who will have the right to forbid, restrict, initiate or require lifelogging? And what of power relations? Won't the powerful become even more powerful if lifelogging can be imposed and lifelogging content may be accessed by others? Who will have the right to access the content of a person's lifelog? What, especially, will be the lifelogging-related entitlements of parents, employers and the government? And what of access by spouses, researchers, business partners, accountants, lawyers and private physicians presumed to have confidential and/or fiduciary relationships with the individual?

Lifelogging preserves individually produced “capta” – capta defined as “units of data that have been selected and harvested from the sum of potential data.”²⁸ Because lifelog data is conceived as self-produced, Dodge and Kitchin have characterized lifelogging as personal “sousveillance”.²⁹ Lifelogging has sousveillance and surveillance dimensions.³⁰ It is sousveillance to the extent that it captures data about oneself or from the perspective of oneself. But it is surveillance to the extent that it is designed to capture data about others, including others who may also be engaged in acts of sousveillance or surveillance. Gordon Bell’s MyLifeBits infrared SenseCam indiscriminately photographs

28 See Martin and Kitchin, ‘Outlines of a world,’ supra note 5 at 432.

29 Id at 434. They borrow the term “sousveillance” from Steve Mann., citing Steve Mann, J. Nolan and B. Wellman, “Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments, 1 Surveillance and Society 331-355 (2003).

30 See Steve Mann’s discussion of the equilibrium between surveillance and sousveillance, <http://wearcam.org/anonequity.htm>, (“Surveillance is derived from French “sur” (above) and “veiller” (to watch). Typically (though not necessarily) surveillance cameras look down from above, both physically (from high poles) as well as hierarchically (bosses watching employees, citizens watching police, cab drivers photographing passengers, and shopkeepers videotaping shoppers). Likewise Sousveillance, derived from French “sous” (below) and “veiller” (to watch), is the art, science, and technologies of “People Looking at”. Sousveillance does not immediately concern itself with what the people are looking at, any more than surveillance concerns itself with who or what is doing the looking. Instead, sousveillance typically involves small person-centric imaging technologies, whereas surveillance tends to be architecture or enviro-centric (cameras in or on the architecture or environment around us). Sousveillance does not necessarily limit itself to citizens photographing police, shoppers photographing shopkeepers, etc., any more than surveillance limits itself along similar lines. For example, one surveillance camera may be pointed at another, just as one person may sousveill another. Sousveillance therefore expands the range of possibilities, without limitation to the possibility of going both ways in an up-down hierarchy. With the miniaturization of cameras into portable electronic devices, such as camera phones, there has been an increased awareness of sousveillance (more than 30,000 articles, references, and citations on the word “sousveillance” alone), and we are ready to see a new industry grow around devices that implement sousveillance, together with a new sousveillance services industry.”).

warm objects in its view, including people. Human individuals live social rather than solitary lives. One person's comprehensive full-life, lifelog would inevitably capture biography and expressions of the lives of other persons. How, if at all, should the capture and surveillance implicit in personal sousveillance be regulated?³¹ How can security against harmful falsification, deletion, data breaches, or identity theft be assured? Would lifelogs turn individuals into surveillance partners of government? How much access should the government have to an individual's lifelog for national security, law enforcement, public health, tax compliance, and routine administrative purposes? The ethical and legal implications of lifelogging merit the serious attention it is beginning to receive.

D. Privacy Concerns

The more comprehensive and continuous the lifelogging, the more significant the ethical and legal problems. Two of the most obvious and important such problems raised by comprehensive, full-life lifelogging are (1) pernicious records, recall, replay and remembrance—for short, pernicious “memory”; and (2) pernicious surveillance. Both involve threats to privacy. Privacy concerns arise because lifelogs are not destined solely for storage until the subject's death like Warhol's cardboard boxes, or sealed for 5,000 years like a World's Fair time capsule. By design, lifelog capta will be accessible and

31 Cf. Philip Agre, *Surveillance and Capture: Two Models of Privacy*, 10 *The Information Society* 101 (1994) (contrasting metaphorical understandings of privacy). A given person may or may not specifically intend “surveillance” and yet collect (“capture”) data of the sort that would result from intentionally spying on others.

useable. Moreover, the act of capturing data itself implicates privacy concerns of all sorts, not just informational privacy and data protection.³² The DARPA LifeLog project was abandoned due to concerns raised about the privacy implications both of the research protocol and the ultimate products of the research.³³ Memory can be a very good thing, but it can also encourage harmfully dredging up or revisiting past conduct. Surveillance can also be a very good thing, but it turns into a social evil when it trains watchful, spying eyes needlessly and hurtfully. First, I will highlight privacy-related and other problems tied to memory; then I will consider privacy-related and other problems connected with surveillance.

1. Pernicious Memory

32 By privacy concerns of all sorts, I mean concerns about access to data/information, people, the attributes of identity, their intimate decisions and relationships—informational, physical, proprietary, decisional, and associational forms of privacy. See Anita L. Allen, *Privacy Law and Society* (2007) ___ ; Anita L. Allen, *Encyclopedia ed* (William Stapleton) (2007)(explaining these distinctions with illustrations.)

33 DARPA modified its original call for proposals to acknowledge research ethics and other ethical, legal and social implications: “The purpose of this modification is to reiterate this requirement and to provide clarification guidance regarding the capture by LifeLog sensors of imagery and audio of people other than the user of the LifeLog system. . . .” LifeLog researchers shall obey all applicable privacy laws and regulations, and shall avoid even the appearance of the invasion of privacy. LifeLog physical data capture systems shall allow the LifeLog user to dynamically activate and deactivate the recording of audio and video, independent of data stream processing such as using optical flow or ambient light and noise to measure motion or transitions between indoors and outdoors. LifeLog researchers shall not capture imagery or audio of any person without that person's a priori express permission. In fact, it is desired that capture of imagery or audio of any person other than the user be avoided even if a priori permission is granted. “ http://www.darpa.mil/ipto/solicitations/closed/03-30_mod3print.htm

It is unclear precisely what lifelogging technology in common usage will be designed to do, precisely how popular it will become, and precisely how people will want to use the data they store.³⁴ But we know already that people are drawn to documenting their experiences, and that nearly everyone has occasionally wished for a better memory.

Lifelogging potentially enhances biological memory by enabling superior, electronic records, replay, recall and possible remembrance. I say “possible” remembrance because encountering a past experience need not cause one literally to remember it. Memory does not work that way. For example, I demand proof to substantiate a friend’s claim that I dressed badly in the 1970s—worse than everyone else. She shows me a photograph that settles the matter: I am standing astride a bicycle wearing a loud Indian print dress with a fringed hemline, argyle socks, wooden sandals and ski glasses. To this day I cannot recall ever donning that tacky get up, hopping on a bike and stopping to chat with a friend carrying a camera. But it happened.

The capacities to recall, to be reminded, and to review records of the past can be valuable. Imagine you are someone who often forgets the details of conversations you are expected to remember. Suppose that you could invisibly record and store conversations in electronic memory for convenient retrieval on demand. You could be spared plenty professional disapproval and social embarrassment. Now imagine that you are a psychotherapy patient trying to gauge the severity of a bout of depression experienced a

34 Cf. Liam J. Bannon, *Forgetting as a Feature, not a Bug: the duality of Memory and Implications for Ubiquitous Computing*, 2 *CoDesign* 3, 4 (2006) (“Examining the ways in which new technologies might augment human and social—and even political—activities in the future is a necessary, yet risky endeavor.”).

few years back. Suppose you could retrieve lifelog data. Your lifelog records and recordings reveal that at times you were irritable and sad, but also that you were at times manic. With the help of the lifelog data, your therapist could confidently diagnose and treat you for a bipolar mood disorder.

Despite practical utility suggested by the foregoing illustrations, electronic memory enhancement is not an unqualified good. Electronic memory enhancement enables destructive reminding and remembrance. The un-redacted lifelog could turn into a bigger burden on balance than fallible biological memory cum conventional contemporary enhancements.

a. Dredging-up the Past

I lose my temper and slap a dear friend at a party. My lifelog records the incident. After making amends and being forgiven, I decide to delete the episode from my log. The technology design allows for this. But a dozen other party guests have captured the slapping incident on their lifelogs, too. Suppose I do not have the technical ability to blot out all of their electronic memories of my misconduct at will. I cannot prevent acquaintances from someday throwing my fault in my face, leaking video evidence of my aggression to a potential lover or employer, and mass communicating my outburst all over the internet. World-wide exposure is a possible outcome of a momentary lapse of judgment. Once a dust bin, history becomes a freezer.

Lifelogging would extend the longevity of personal misfortune and error. Not only might an individual's own lifelog problematically preserve a record of bad luck and mistake, the lifelogs of others with whom the individual has come into contact might do the same. Yet people typically have a legitimate moral interest in distancing themselves from commonplace misfortunes and errors.³⁵ In order to create that distance, they need to be safe from memory: they need to forget and need others to forget, too.³⁶

Dredging-up the past can hurt feelings, stir negative emotions, and ruin lives. We can see clearly the potential cruelty and harmful consequences of resurrecting the past in the fact patterns of a familiar line of privacy tort cases.³⁷

Melvin v. Reid pitted a homemaker, who had once been a prostitute wrongly accused of murder, against filmmakers who used her actual maiden name in "The Red

35 Uncommon errors, such as perpetrating large scale human rights atrocities are another matter. I do not think Adolph Hitler had a moral interest in distancing himself from his role in the Holocaust.

36 Some people will be better able –and more disposed--to accept and offer forgiveness than others, no matter how vivid the memories to which they have access.

37 The "dredging-up the past" cases I have in mind date back to the 1930s. See *infra* notes 32-35. Some of the more recent cases in the line include *Hall v. Post*, 323 N.C 259 (NC 1988) (no liability for publishing story about a woman who many years earlier had been married to a carnival barker and abandoned their child); *Uranga v. Federated Publs.*, 138 Idaho 550 (Id. 2003) (no liability for re-publication of a forty year old court record associating the plaintiff with homosexuality); and *Willan v. Columbia County C.A.* 7 (Wis.) 2002 (no liability where police queried computerized database maintained by the FBI's National Crime Information Center and discovered that mayoral candidate had been convicted of felony burglary in 1980's in another state).

Kimono”, a movie based on her life.³⁸ The Melvin court held that the policy interest of the state in rehabilitation justified allowing the woman’s privacy suit to stand.³⁹ One of the most intriguing privacy tort cases of all time went the other, more typical, way. William James Sidis brought a lawsuit against the New Yorker magazine after a reporter weaseled into his apartment for an interview and then published a story that belittled Sidis’ eccentricities and shabby circumstances.⁴⁰ Mr. Sidis had been a celebrated child-

38 Melvin v. Reid, 112 Cal. App. 285 (Cal. Ct. App. 1931) (“The use of appellant’s true name in connection with the incidents of her former life in the plot and advertisements was unnecessary and indelicate and a willful and wanton disregard of that charity which should actuate us in our social intercourse and which should keep us from unnecessarily holding another up to scorn and contempt of upright members of society.”)

39 But see, Willan v. Columbia County C.A.7 (Wis.) 2002 (“Anyway the Melvin case, paternalistic in doubting the ability of people to give proper rather than excessive weight to a person’s criminal history, is dead, see, e.g., Rawlins v. Hutchinson Publishing Co., 218 Kan. 295, 543 P.2d 988, 993-96 (Kan.1975); Barbieri v. News-Journal Co., 189 A.2d 773, 776-77 (Del.1963); Jones v. New Haven Register, Inc., 46 Conn.Supp. 634, 763 A.2d 1097, 1100-03 (Conn.Super.2000), killed by Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 494-96, 95 S.Ct. 1029, 43 L.Ed.2d 328 (1975); see Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1230-32 (7th Cir.1993); Romaine v. Kallinger, 109 N.J. 282, 537 A.2d 284, 292-95 (N.J.1988); Montesano v. Donrey Media Group, 99 Nev. 644, 668 P.2d 1081, 1086-88 (Nev.1983); McCormack v. Oklahoma Publishing Co., 613 P.2d 737, 741-42 (Okla.1980); Rawlins v. Hutchinson Publishing Co., *supra*, 543 P.2d at 995-96; Pemberton v. Bethlehem Steel Corp., 66 Md.App. 133, 502 A.2d 1101, 1118-19 (Md.Spec.App.1986); Shulman v. Group W. Productions, Inc., 18 Cal.4th 200, 74 Cal.Rptr.2d 843, 955 P.2d 469, 500-01 (Cal.1998) (concurring opinion). The Supreme Court held in Cox that the First Amendment creates a privilege to publish matters contained in public records even if publication would offend the sensibilities of a reasonable person. (The matter in question was the identity of a woman who had been raped and murdered.) See also Florida Star v. B.J.F., 491 U.S. 524, 537-38, 109 S.Ct. 2603, 105 L.Ed.2d 443 (1989).”).

40 Sidis v. F-R Pub. Corp. 113 F.2d 806 (2d Cir. 1940) (New Yorker article about former prodigy was ‘merciless’ and ‘ruthless’) (“Regrettably or not, the misfortunes and frailties of neighbors and ‘public figures’ are subjects of considerable interest and discussion of the rest of the population. When such are the mores of the community, it would be unwise for a court to bar their expression in the newspapers, books, and magazines of the day.”)

prodigy, the youngest person ever to attend Harvard, and a college graduate by age 16. Stressing the enormity of his past fame, the court held that a magazine story describing his descent into obscurity was newsworthy. A case of the same ilk, Briscoe v. Reader's Digest Ass'n, was brought by a convicted armed hijacker, turned solid citizen and parent, who sued a newspaper for publishing a reference to his crime.⁴¹ The court left it to a jury to decide whether the hijacker's past was newsworthy. In all three cases, someone suffered humiliation and loss of standing in the community because someone else chose to bring up—the victims might say, dredge up—the truths of their pasts.

Current interpretations of tort law do not favor granting relief under privacy tort theories to people whose once-public pasts have been resurrected by the media for public comment and discussion. The First Amendment and the common law mandate wide freedom for speaking truth, accurate news reporting and artistic expression. Yet, wherever the seclusion and private facts remedies appear on the books, a doctrinal framework for tort liability for lifelog-based disclosures is in place.⁴² The crucial inquiry is whether judges and juries examining the facts would be likely to find that a lifelog data

41 Briscoe v. Reader's Digest Ass'n, 4 Cal.3d 529 (Cal 1971) (“A jury might well find that a continuing threat that the rehabilitated offender's old identity will be resurrected by the media is counterproductive to the goals of [rehabilitation].”).

42 North Carolina rejected the private fact tort in Hall v. Post, 323 N.C. 259 (N.C. 1988) (“We conclude that any possible benefits which might accrue to plaintiffs are entirely insufficient to justify adoption of the constitutionally suspect private facts invasion of privacy tort which punishes defendants for the typically American act of broadly proclaiming the truth by speech or writing. Accordingly, we reject the notion of a claim for relief for invasion of privacy by public disclosure of true but "private" facts.

disclosure was “highly offensive to a reasonable person” and not newsworthy or otherwise of “legitimate interest to the public.”⁴³

It is not utterly inconceivable that a state court could find a defendant liable under the intrusion or public disclosure of private fact torts for dredging-up the past. The best case for liability would involve publication of information about a solitary private person secreted in his or her own lifelog or covertly captured in the lifelog of a trespassing spy (e.g., images of the person, depressed and weeping alone in front of a mirror in the bathroom). The lifelog technology imagined for the near future captures streams of shared experience, not the stream of consciousness. Embarrassing and humiliating lifelog recordings made at group events or in public places might fail to meet the standard of “highly offensive to a reasonable person” in any court. There is a strong, if misguided, tendency in U.S. law to discount the significance of privacy in public.⁴⁴

43 See Restatement of Torts (Second) Section 652 (B) and 652D (a) and (b) (emphasis added):

652B. Intrusion upon Seclusion

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

652D. Publicity Given to Private Life

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

44 See Anita L. Allen : Uneasy Access (1988). H Nissenbaum, "[Protecting Privacy in an Information Age: The Problem of Privacy in Public,](#)" Law and Philosophy, 17: 559-596, 1998.

It is worth asking whether it is ethical for would be truth-tellers protected by the First Amendment and common law to stand on their rights, knowingly wounding people who are trying to forget their pasts.⁴⁵ To get at an answer, consider what, if anything, made the plaintiffs' privacy claims in Melvin, Sidis and Briscoe ethically plausible. Why might an ethical truth-teller have even considered forbearance? Where was the harm, unfairness or failure of character in doing what the law may or may not have allowed? To be sure, the unflattering information was archived in media and public records. But most people did not have the information the plaintiffs wished to hide at all or at their fingertips. It would have taken some dredging to get it. That the information was not readily accessible to others, fostered in the plaintiffs expectations of privacy and secrecy around which they built their interpersonal relationships. This was especially true of the

45 The ethical code promulgated by the Society of Professional Journalists exhorts journalists to respect interests in seclusion, anonymity and informational privacy as species of minimizing harm:, see <http://www.spj.org/ethicscode.asp>:

“Journalists should:

...— Show compassion for those who may be affected adversely by news coverage. Use special sensitivity when dealing with children and inexperienced sources or subjects.

— Be sensitive when seeking or using interviews or photographs of those affected by tragedy or grief.

— Recognize that gathering and reporting information may cause harm or discomfort. Pursuit of the news is not a license for arrogance.

— Recognize that private people have a greater right to control information about themselves than do public officials and others who seek power, influence or attention. Only an overriding public need can justify intrusion into anyone's privacy.

— Show good taste. Avoid pandering to lurid curiosity.

— Be cautious about identifying juvenile suspects or victims of sex crimes.

— Be judicious about naming criminal suspects before the formal filing of charges.

— Balance a criminal suspect's fair trial rights with the public's right to be informed.”

Cf. See Anita L. Allen, Why Journalists Can't Respect Privacy, in *Journalism and the Debate Over Privacy* (ed). Craig LeMay (2003) (observing the demise of the privacy-protection norms among practicing journalists and explaining the practical limits on privacy protection.).

plaintiffs in Briscoe and Melvin, neither of whom had every experienced national celebrity. With ready access to news archives, the New Yorker performed an easy dredge, a bit of investigative journalism, and then released information about Sidis into the world. The harm to him was shame, distortion and unwanted attention, as information flowed beyond preexisting “social networks”.⁴⁶ The New Yorker violated “norms of appropriateness” by using deception to gain fresh access to Sidis, and norms of fair information “distribution” when it republished facts about Sidis younger people did not know and most older people had forgotten.⁴⁷

b. The future of “the Past”

The limitations of memory combined with practical barriers to efficient dredging once made it rational to predict that much of the past could be kept secret from people who matter. And three short decades ago, reliance on expectations of substantial privacy about the past were highly reasonable. One could build a new life on a premise of de facto concealment. One could earn trust and honor. One could walk with dignity before others. Respecting expectations of privacy about the past in a world of mere human

46 See Lior Jacob Strahelivitz, A Social Networks Theory of Privacy, 72 U. Chi. L. Rev. 919 (2005) (“Where a defendant’s disclosure materially alters the flow of otherwise obscure information through a social network, such that what would have otherwise remained obscure becomes widely known, the defendant should be liable for public disclosure of private facts.”)

47 See also Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119, 136-143 (2004) (distinguishing norms of appropriateness and distribution norms for information disclosures).

memory and mostly paper archives was an obligation that ethical principles of care and character would surely dictate.⁴⁸

The Supreme Court drew a parallel conclusion about legal obligations and legal principles. In an oft-cited case, the Court interpreted the Freedom of Information Act's privacy exemptions to protect individuals from the federal government releasing their criminal "rap sheets" to the media.⁴⁹ Criminal histories are public data, the court argued, but data that ordinarily enjoys "practical obscurity."⁵⁰ Thus "[t]he privacy interest in maintaining the practical obscurity of rap-sheet information will always be high."⁵¹

48 But see H.J. McCloskey, *The Political Ideal of Privacy*, *The Philosophical Quarterly*, Volume 21, Issue 85 (October, 1971), 303-314, arguing on ethical grounds that a man has a right to know if the woman he is thinking of marrying had been married before or once gave birth to a child. McCloskey argues that loving relationships create obligations of accountability. I agree with the principle that there may be relationships or categories of relationships in which secrecy about significant past behavior is ethically unacceptable.

49 *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 US 749, 771 (1989) (FOIA "[e]xemption 7(C), by its terms, permits an agency to withhold a document only when revelation 'could reasonably be expected to constitute an unwarranted invasion of personal privacy.' . . . The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded.").

50 *Id.* at 780 ("Finally: The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of "what the Government is up to," the privacy interest protected by Exemption 7(C) is in fact at its apex while the FOIA-based public interest in disclosure is at its nadir.").

51 *Id.* at _780_.

In an era of electronic archives, traditional predictions and expectations of privacy about the past have begun to look less reasonable. The changed social context – we are now in an “information age”—works against former celebrities and felons hoping to conceal past fame or infamy. Information about the past is ready at hand. Much of the focus of information science is on how to eliminate practical obscurity through electronic archive and retrieval. Electronic accessibility renders past and current events equally knowable. The very ideas of “past” and “present” in relation to personal information are in danger of evaporating. The past is on the surface, like skim. A former mayoral candidate unsuccessfully sued after police queried a computerized database maintained by the FBI's National Crime Information Center and learned the he had been convicted of felony burglary in 1980's in another state⁵² There is much less “dredging” to get to the past; only pointing and clicking to achieve replay.

Today's “Sidis” knows that anyone can access online data bases to learn about others' achievements, misfortunes, crimes, employment, affiliations, and publications. Curious neighbors or the media might Google Sidis for purposes unrelated to his interesting past, discovering inadvertently, in an instant, that he had been an acclaimed child prodigy deemed to have a bright future.

Information about ordinary people travels from the offline world onto cell-phone cameras, onto Youtube, television talk shows, and Google. Today's “Melvins” and “Briscoes” must expect their crimes to have a rich afterlife, not only in newspapers and

⁵² See, e.g., *Willan v. Columbia County C.A.7* (Wis. 2002).

government records, but in videos, telephones, web logs, twitter.com, facebook.com and myspace.com, as well. Whole television programs are based on video of crimes being committed—robberies, shootings, high speed chases, sexual predation and criminal solicitation.⁵³ The 2007 Virginia Tech campus massacre⁵⁴ was documented in video and audio recordings made by Swedish exchange students, wounded victims and by the suicidal murderer himself.⁵⁵ These made their way onto television and the web.

As privacy and concealment become more difficult to obtain, they may come to matter less or differently. In a universe of cheap, massive lifelog data retention, individuals would perhaps come to understand digital capture and unwanted data disclosure as mundane risks, like swallowing bugs at a picnic. More radically, they may come to understand themselves, not as longitudinal well-integrated personalities but as ever-present navigable data streams no one fully controls.

Passwords, encryption, and other security measures will help to keep lifelog capta private. But social norms may fail to ascribe individuals the right to keep their own lifelogs sufficiently private from family and friends to securely protect their emotional

53 Deborah Jermyn, *Crime Watching: Investigating Real Crime TV* (2006).

54 Alessandra Stanley, [Deadly Rampage and No Loss for Words](#), *New York Times*, 4/17/07 A19 .

55 See [The Massacre at Virginia Tech - Part 2](#), CNN NEWS Author: Howard Kurtz, Soledad O'Brien; 4/22/07 CNNNEWS (No Page) 2007 WLNR 7596930. The experience of the Swedish exchange students is reported at <http://www.handelskammaren.net/item.aspx?id=4891>.

lives and careers. And in any case, unless lifelog design moves in a very different direction than the MyLifeBits prototype, individuals will be featured in other people's lifelogs, probably without a legal right to fully control how the data about them is used, shared or construed.⁵⁶ Existing state and federal wiretapping laws limit the right of law enforcers and private citizens alike to audio-record conversations without the consent of at least one party.⁵⁷ But videotaping is less stringently regulated, and videotaping in public places, short of upskirting, harassment or stalking, is rarely unlawful.⁵⁸

Lifelogs will be downplayed by some technology enthusiasts, as an incremental rather than a revolutionary change in the capacity to do what used to be called dredging up the past. Yet the change in data retention practices widespread lifelogging would entail would be revolutionary. It is mainly the deeds of people of celebrity or accomplishment that are amenable to discovery or recall with the help of an internet search engine or media archive. But lifelogging means the deeds of just about anyone can be stored, recalled and shared by others who get their hands on the files.

56 The suggestion has been made that wearable anti-data capture technologies will be developed that can block the ability of other people's lifeloggers to record one's activity. See Total Recall

57 Cf. *Moore v. Telfon Communications*, 589 F.2d 959 (9th Cir. 1978) (federal wiretap act prohibits nonconsensual recording of telephone call, but permits private individual to make recording of attempted extortion).

58 Cf. *U. S. v. Torres*, 751 F.2d 875 (7th Cir. 1984) (videotaping not governed by federal wiretap act, but Fourth Amendment considerations may apply).

Again, technologies are making the past easily and eternally present. There is no onerous dredging, no “practical obscurity” sheltering scattered facts. Full-life lifelogging will likely lead to unwanted data collection, retention and disclosures that may not be considered tortious or otherwise unlawful under existing privacy law. And they might not even strike most people as unethical. Since the primary purpose of lifelogs will not be to destroy other people’s lives but to archive personal experience, it is unlikely at this juncture that innovators, consumers or policy makers will view the emotional injury and privacy invasion concerns raised by the technology as grounds for its suppression. It is desirable, though, that the technology and the social practices that surround its use take appropriate account of the problems in living that can stem from bringing up the past.

2. Mental and Moral Health Hazards

Improvements in mental health diagnosis could flow from the accessibility of lifelog data. Finally therapists could see and hear the behavior of clients not sick enough for monitoring in a hospital. Therapists would have the equivalent of the Holter Monitor ambulatory electrocardiograph machine that cardiologists employ to detect subtle heart disease. Yet the vivid recall lifelogs will permit might turn out to be a psychological hazard.⁵⁹ The lifelogging concept is insensitive to the therapeutic value of forgetting the

59 Cf. *Oblivion*, Marc Auge [accent over e], translated by Marjolijn de Jager, *Oblivion* Minneapolis, University of Minnesota Press at 3 (“One must know how to forget in order to taste the full favor of the present, of the moment, and of expectation...”)

details of experience.⁶⁰ Trauma often needs to recede into near oblivion. Rumination about the past may need to be discouraged to make room for fresh experiences and perspectives.

Lifelogging operates with a bias in favor of memory and the capacity for detailed recall of the past. Lifelogging designers may be thinking “documentary film” rather than “interpretative diary”. Will lifelogs allow the individual to mold and change her identity? A person who has been successfully treated for post traumatic stress syndrome after returning from a bloody war may benefit from memories that have faded. A person who had come to terms with a childhood of sexual molestation may benefit from the loss of painful memories.⁶¹ After sex-reassignment, a person might wish to break with aspects of the opposite-sexed prior self. There may be an easy technological fix for this problem. Design the logging devices to allow people to turn them off in potentially trauma-inducing settings. Enable deletion of painful or dysfunctional recordings that have outlived their usefulness to the individual.

60 See <http://www.webmd.com/anxiety-panic/features/forget-something-we-wish-we-could>

61 Cf. Adam J. Kolber, Therapeutic Forgetting: The Legal and ethical Implications of Memory Dampening, 59 Vand. L. Rev. 1561 (2006) (pharmacological memory dampening may be warranted as treatment for trauma victims, and should not be avoided out of blind bias in favor of natural cognitive abilities).

Another psychological hazard is harder to fix: voluntary, but pathological rumination.⁶² The technology will enable excessive rumination by persons experiencing unipolar or bipolar depression.⁶³ The depressed individuals might constantly revisit and reify their repository of perceived errors, slights, lost opportunities and injustices. The therapist may find it especially difficult to persuade a patient that lifelogger data are not fixed, “hard” evidence of an important whole story, rather than as something partial, ambiguous, unimportant and interpretable.

Rumination and stress are not the only mental health related concerns. Persons affected by mental illness sometimes commit acts of horrific unkindness and violence when they are ill, for which they are sorry and the people they harm are willing to forgive.⁶⁴ But how useful is forgiveness when there is a diminished capacity to forget?

Indeed, the ability to move on from wrong doing is something even wrongdoers not affected by mental illness may find it hard to do in a world of lifeloggers. The expectation that lifeloggers delete memories of offensive conduct for which others have forgiven them might someday emerge. My deleting data about my forgiven offenses from

62 Ellen McGrath, The Rumination Rut, Psychology Today, <http://psychologytoday.com/articles/pto-2687.html>. See also [Addis, M E; Carpenter, K M](#), Why, why, why?: Reason-giving and rumination as predictors of response to activation- and insight-oriented treatment rationales. 55 J Clin Psychol. 881-94 Jul (1999).

63 A person predisposed to ruminate, may do so excessively whether her memory bank is vast or nearly vacant. My speculation is that a culture of memory machines may exacerbate problems of pathological rumination.

64 See e.g., Kay R. Jamison, The Unquiet Mind (1995), 120-122 (bipolar professor of psychiatry describes the violence, remorse and forgiveness precipitated by her own mental illness).

my lifelog may have less value, though, if the others around me do not delete their records of what I have done. But incomplete networking and communication means that information of about wrongs will not be consistently followed up with information about moral repair. Another difficulty: asymmetry. The forgiven offender may be best served by data deletion, while the forgiving victim may be best served by data preservation. Some people are too forgiving of domestic violence, harassment and the like. It might be a good idea to replay the tapes, as it were, to spur caution. Victims may have a complex ethical duty to retain but secret lifelog data of forgivable forgiven wrongs.

2. Pernicious Surveillance

I now turn from pernicious memory to pernicious surveillance. Lifelogs could someday become exceedingly comprehensive and sensitive windows into a person's life. They may be stored on standalone personal computing devices only; or uploaded to the internet for more permanent and secure storage. They may be included in medical records, shared with friends and aggregated with the lifelogs of others.

A great deal of data is already collected and retained about individuals, some by the individual, some by others. In the future the need for personal lifelogging could be tempered by the fact that business and government will routinely and systematically collect detailed data about individuals for purposes of marketing, security and social control. Moreover, because sousveillance is also surveillance, lifeloggers join the state and industry as fellow people-watchers.

A lay person or surveillance professional could elect to share life-log data featuring the conduct of others. The potential thus exists for using lifelog pervasive computing technology for purposes of spying on others.⁶⁵ To “spy” is to monitor or investigate another’s beliefs, intentions, actions, omissions, or capacities, as revealed in otherwise concealed or confidential conduct, communications and documents. Spying involves covert activity, though not necessarily lies or fraud. Although some spying is virtuous rather than unethical, spying inherently involves taking advantage of those who place their confidence in the social norms that shape a cooperative communal life.⁶⁶ Spying should be presumed wrong because it often uses secrecy to unfair advantage and interferes with the enjoyment of beneficial modes of personal privacy that individuals expect others to respect. Yet there are exceptions to the anti-spying principle: spying on others is ethically permissible, even mandatory, in certain situations, where the ends are good.

Spying is sometimes prompted by genuine obligations of caretaking, such as monitoring an aging adult parent or teenager. Spying may be a way to prove a humiliating adultery, gather evidence against a corporate crime, or expose a terrorist. Where spying is ethically permitted or required, there are ethical limits on the methods of spying. The virtuous spy will violate privacy and transparency norms, but he or she will,

65 Cf. Jeffrey A. Lowe, Big Brother Will Be Watching: Lifelog Project Up Administration’s Sleeve Threatens Privacy Rights of Every American, L.A. Daily J., July 21, 2003), at 6, cited in Oliver Ureland and Rachel Howell, The Fear Factor: Privacy, Fear and the Changing Hegemony of the American People and the Right to Privacy, 29 NCJILCR 671 (2004), n. 4.

66 Anita L. Allen, The Virtuous Spy, __ Monist __ (2008).

to the extent possible, continue to act with respect for the moral autonomy and for the moral and legal interests of the investigative target.⁶⁷ This value attached to spying thus provides no justification or defense for recreational spying, whether using life-log technology or more traditional means. Widespread lifelogging could increase the amount of illicit, unethical recreational surveillance to intolerable levels.

There is no reason to think lifelogs will be immune from government access or surveillance. On the contrary, there is every reason to think lifelogging will be a boon to the legal system and government surveillance. The sousveillant will be the true sibling of Big Brother. I reach this conclusion by taking notice of the spirit and letter of current federal surveillance policy. Current laws give the government access to virtually all means of communications and data storage. A government that has traditionally enjoyed access to communications and correspondence will want access to lifelogs. Diaries are not off limits,⁶⁸ and my prediction is that lifelogs will not be treated more favorably.

The Supreme Court has held that the Fourteenth Amendment protects information privacy, but in a case that is seldom applied.⁶⁹ Federal law and policy affirm the concept of search and seizure based on warrants and individualized suspicion, while allowing

67 Anita L. Allen, *The Virtuous Spy*, __ *Monist* __ (2008).

68Cf. *People v. Miller*, Cal.App., 60 Cal.App.3d 849, 866-67 (1976) (“Contrary to defendant’s contention, evidentiary use of the diary did not violate the constitutional privilege against self-incrimination. The privilege does not prevent the otherwise lawful seizure of a document even when its contents are communicative. ([Andresen v. Maryland \(1976\) 427 U.S. 463, 96 S.Ct. 2737, 48 L.Ed.2d -- \(44 U.S. Law Week 5125\)](#); [United States v. Dawson \(9th Cir. 1975\) 516 F.2d 796, 806](#); [United States v. Bennett, supra](#), 409 F.2d at p. 896; see also, [People v. Thayer \(1965\) 63 Cal.2d 635, 638, 47 Cal.Rptr. 780, 408 P.2d 108.](#))”).

69 See *Whalen v. Roe*, 429 589 (1977).

numerous exceptions in Fourth Amendment law, such as the “special needs” exceptions.⁷⁰ Although the Electronic Communications Privacy Act (1986) enhances Fourth Amendment protections, it regulates government access to communications, stored data and communications transactions records without barring access.⁷¹ The Foreign Intelligence Surveillance Act also regulates rather than prohibits access to premises, tangible items and communications.⁷² With National Security Letters the government can subpoena business records, and could presumably subpoena lifelog data from private businesses set up to systematize, transfer or back-up lifelog data.⁷³

Designing the government out may not be a realistic option for technology innovators. In the 1990’s industry effectively blocked full implementation of the Clipper

70 Cf. [Samson v. California](#), 126 S.Ct. 2193 (2006) (Fourth amendment permits search of parolee without warrant or special needs exception).

71 The Electronic Communications Privacy Act of 1986 (ECPA) Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, [18 U.S.C. § 2510](#)).

72 The Foreign Intelligence Surveillance Act (FISA) of [1978](#), as amended by Section 215 of the USA Patriot Act (2001), reauthorized 2006.

73 A National Security Letter is a secret administrative subpoena used by the FBI to obtain information in private hands without obtaining a search warrant. As described by the FBI, “A National Security Letter (NSL) is a letter request for information from a third party that is issued by the FBI or by other government agencies with authority to conduct national security investigations. “ See http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm (“NSL authority is provided by five provisions of law: The Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5), for financial institution customer records; the Fair Credit Reporting Act, 15 U.S.C. § 1681u(a) and (b), for a list of financial institution identities and consumer identifying information from a credit reporting company; the Fair Credit Reporting Act, 15 U.S.C. § 1681v, for a full credit report in an international terrorism case. This provision was created by the 2001 USA PATRIOT Act; the Electronic Communications Privacy Act, 18 U.S.C. § 2709, for billing and transactional communication service provider records from telephone companies and internet service providers; and the National Security Act, 50 U.S.C. § 436, for financial, consumer, and travel records for certain government employees who have access to classified information.”).

Chip concept of government access to encrypted data.⁷⁴ Yet, federal policy reflects the notion that new communications technology sign must allow for government access and surveillance. This is the spirit of CALEA, the Communications Assistance for Law Enforcement Act (1994).⁷⁵ CALEA compels the private sector to insure that new communications technologies do not thwart law enforcement and its reach was recently extended to govern aspects of voice over internet protocol technologies.⁷⁶ While data

74 President Bill Clinton's White House announced the Clipper Check Program in 1993. See http://www.epic.org/crypto/clipper/white_house_statement_4_93.html As described by the Electronic Information Privacy Center, <http://www.epic.org/crypto/clipper/> :

“The Clipper Chip is a cryptographic device purportedly intended to protect private communications while at the same time permitting government agents to obtain the "keys" upon presentation of what has been vaguely characterized as "legal authorization." The "keys" are held by two government "escrow agents" and would enable the government to access the encrypted private communication. While Clipper would be used to encrypt voice transmissions, a similar chip known as Capstone would be used to encrypt data.”

“The underlying cryptographic algorithm, known as Skipjack, was developed by the [National Security Agency \(NSA\)](#), a super-secret military intelligence agency responsible for intercepting foreign government communications and breaking the codes that protect such transmissions. In 1987, Congress passed the [Computer Security Act](#), a law intended to limit NSA's role in developing standards for the civilian communications system. In spite of that legislation, the agency has played a leading role in the Clipper initiative and other civilian security proposals, such as the [Digital Signature Standard](#).”

75 See Communications Assistance for Law Enforcement Act of 1994 (CALEA). See also website of the Federal Communications Commission, <http://www.fcc.gov/calea/> (“In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities.”)

76 CALEA extended to voice over internet, see <http://www.fcc.gov/calea/> 2007.

destruction is a command of at least one federal privacy statute,⁷⁷ the federal government has sought to discourage automatic destruction of its own administrative records.⁷⁸ The

77 Video Privacy Protection Act 18 U.S.C. § 2710 et seq. “(e) Destruction of Old Records -- A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b) (2) or (c) (2) or pursuant to a court order.”

78 The federal government has complex record creation, disposal and preservation guidelines. See <http://www.archives.gov/records-mgmt/faqs/general.html> (frequently asked questions and summaries of policies on official U.S. cite). Cf. Sue Dill Calloway’s summary of federal document retention rules applicable to private sector at <http://www.hipaadvisory.com/regs/recordretention.htm>:

“There are a number of other record keeping laws required by the federal laws that have specific record-keeping requirements. These are as follows:

Fair Labor Standards Act: The Department of Labor requires employers to comply with several record-keeping regulations related to wages, hours, sex, occupation, condition of employment for three years. This concerns records containing employment information, payroll, and certificates and for two years of basic employment and earning records, wage rate tables, work time schedules, order shipping and billing records, job evaluations, merit seniority systems and other documents that explain wage differences to employees of the opposite sex in the same establishment. This also includes any deductions from or additions to pay. (29 CFR 516.2-516.6 and 516.11-29).

Occupations Safety and Health Administration (OSHA): OSHA requires employers to keep records of both medical and other employees who are exposed to toxic substances and harmful agents. Employers must maintain these records for 30 years.

Health and Human Services: Hospitals that participate in Medicare must keep medical records on each inpatient and outpatient, records of radiologic service, nuclear medicine including records for the receipt and disposition of radiopharmaceuticals for five years. (42 CFR 482.24, .26, and .53). Psychiatric hospitals must maintain special records including development of assessment/diagnostic data, treatment plan, record progress, discharge planning, and discharge summary for 5 years.

Health and Human Services: Facilities certified as comprehensive outpatient rehabilitation facilities (CORFs) under the Medicare program must maintain clinical records to justify the diagnosis and treatment plan. These must be maintained for 5 years after the patient is discharged. (452 CFR 485.60).

Health and Human Services: Rural Health clinics that qualify for Medicare and Medicaid reimbursement must maintain medical records for at least six years from the date of the last entry. This retention period is longer in some states because they have a specific statute.

government has moved against the destruction of library⁷⁹ and internet service provider (ISP) records.⁸⁰ The trend in Europe favoring mandatory private sector data retention is unlikely to remain on sister shores.⁸¹

Health and Human Services: Nursing facilities must retain records for clinical records for five years from discharge if no state requirement. The medical records of minors must be kept for three years after they reach the age of majority. (42 CFR 483.75).

Health and Human Services: There are other many specific record retention requirements for various programs administered by the Public Health Service under 42 CFR, such as: Institutions receiving grants for research projects (52.8), Public or not for profit hospitals or schools receiving National Heart, Lung, and Blood institute grants under the National Cancer Research Demonstration Center. (52.8), and Agencies receiving National Institute Grants (526.6).

Internal Revenue Service (IRS): Facilities should keep copies of employment tax records (Social Security documents) for four years after the due date of the tax. If a claimant files a claim, it should be for four years after the date of the filing. (26 CFR 31.6001).

Food and Drug Administration (FDA): Investigators of new drugs are required to keep records to show they did not discriminate against workers because of their age. (29 CFR 1627). Records of each employee with addresses, occupation, date of birth, and compensation earned must be kept for three years. Personnel records related to job applications such as promotion, physical examination results, aptitude tests, and advertisements have to be kept for one year.

Employers Retirement Security Act: Any hospital or employer that has an employee benefit or pension plan must file a summary of the plan with the Department of Labor under the Employee Security Act of 1974 and keep records for not less than six years. (29 USC chapter 18).

Welfare and Pension Plans Disclosure Act: Records must be kept for five years as required under this act for reports under the Welfare and Pension Plan. (29 USC 308).

Federal Employee's Compensation Act: Hospitals and doctors who treat patients covered by this act must keep records of all injury cases including history, description of the injury, degree of disability, x-ray findings, treatment provided and other essential information. (20 CFR 10.410). This federal law only requires what information must be retained but not for how long.

Civil Rights Act and Equal Pay Act: Any employers that are covered by this act must maintain employment and personnel records of hiring, promotion, demotion, termination, transfer, layoff, pay raises, et al for six months from the making of the record of personnel action involved. They must be maintained until final disposition of any discrimination case. (29 CFR 1602.14).

79 See <http://www.ala.org/ala/oif/ifissues/fbiyourlibrary.htm#news> (discussing government efforts to obtain access to library records, bookstores and internet trials)

3. Avoiding Memory and Surveillance: Some Proposals

Martin Dodge and Rob Kitchin examined the ethics of lifelogging and came up with an ironic solution to the problems of psychologically risky mechanical sousveillance and sousveillance-aided government surveillance: infuse lifelogging systems with “imperfection, loss and error.”⁸² The developers of MyLifeBits have also broached this possibility, to reduce the attractiveness of lifelogs to the government.⁸³

80 See James Plummer, "Data Retention": Costly Outsourced Surveillance, Issue #99 January 22, 2007, see <http://www.cato.org/tech/tk/070122-tk.html> (“The Justice Department has been beating the drums since last spring for a “data retention” law that would require Internet service providers to warehouse records of their customers’ online activity for the convenience of government investigators. Most recently, FBI Director Robert Mueller called for such a measure at a law-enforcement convention last October. But the idea has found vocal proponents on both sides of the aisle. Data retention may rear its head again in the 110th Congress.”). See also Goggle, [Taking Steps to further Improve Our Privacy Practices](http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html) , 3/14/2007 03:00:00 PM, <http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html> (“Today we're pleased to report a change in our privacy policy: Unless we're legally required to retain log data for longer, we will anonymize our server logs after a limited period of time. When we implement this policy change in the coming months, we will continue to keep server log data (so that we can improve Google's services and protect them from security and other abuses)—but will make this data much more anonymous, so that it can no longer be identified with individual users, after 18-24 months.”)

81 On March 15, 2006 the European Union adopted Directive 2006/24/EC, mandating "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC" for a period of up to two years. The Directive covers all telephony (land, cell, internet) and internet communications (email).

82 Supra note __, Dodge and Kitchin.

83 Supra note __, New Yorker Magazine.

Dodge and Kitchin reject “the aim of pervasive computing enthusiasts to create a unified, autobiographical (first person) lifelog for each individual through digital technologies that are always on, communicate with each other without human instruction or invention, and are so pervasive that they cover all aspects of human activity and become so banal as to be seemingly invisible”⁸⁴ They embrace a modified conception of lifelogs. The life-logs they embrace would be owned by the individual adult subject. But since ownership cannot guarantee control and the assurance of only personal uses, they propose to make them less functional.

To reduce the incentives for others (including the government) to seek access to individuals’ life-logs, Dodge and Kitchin propose designing lifelogs to function imperfectly, not unlike biological memory. In particular, they propose that the devices have the capacity to “block” recording of some details, “forget” details over time, and “tweak” memory of the past by mis-recording precisely when, where and how certain events took place.⁸⁵ Fallibility of the lifelog will benefit the individuals who own it, too. Free from an “unforgiving” and “merciless” memory machine, persons can “evolve their social identities, live with their conscience, deal with their demons, move on from their past to build new lives, reconcile their own paradoxes and contradictions, and be part of society”.⁸⁶ The Dodge-Kitchin solution works well only if all lifelogs are designed with the features they recommend. Otherwise, a best friend’s or spouse’s lifelog might provide

84 Id. at 7.

85 Id. at 16.

86 Id. at 17, with elisions.

the sort of veridical evidence for a government investigation that one's own lifelog has been designed to thwart. A world in which only the fallible, fading, reality tweaking version of the lifelog is in circulation, is a more "private" world than the world in which veridical loggers are also in use.

There is still time to optimally design full-life lifelogging products. Consumers are not yet clamoring for "perfect" memory full-life life loggers. But given the choice between a Dodge-Kitchin lifelogger and a veridical Total Recall lifelogger, I suspect most consumers would go for the latter, despite the attendant problems of privacy. If Jim and Jill are sentimental lovers who first met at Starbucks on a Tuesday morning, they will not want their lifelogs to have created both inaccurate and inconsistent accounts of their fateful encounter. The "unforgiving" and "merciless" veridical lifelog technology will have gargantuan appeal to consumers, the government, and the health, research and commercial sectors. One's physician cannot be helped with data about blood pressure and heart-rate that may be accurate, but, then again, may be not. The precise color of the item you purchased at Target and the date are the sort of precise, accurate data the commercial sector wants to collect.

Designers of the "Total Recall" veridical lifelog technology, believe its "high level goal is to improve quality of life."⁸⁷ They recognize the privacy issues raised by

87 .C. Cheng, L. Golubchik, and D.G. Kay, "Total Recall: Are Privacy Changes Inevitable?," Proc. First ACM Workshop on Continuous Archival and Retrieval of Personal Experiences, ACM Press, 2004, pp. 86-92; <http://bourbon.usc.edu/iml/recall/papers/>.

the continuous environmental recording aspect of Total Recall. They have even considered the possibility that lifelogging recording technology might violate wiretapping laws, other privacy statutes or fair information practice consent standards. But they seem to find solace in their observation that people in public places lack “reasonable expectations of privacy.”⁸⁸ They do not have much to say about how people should be expected to cope, individually or as a community with “a qualitative change in the heretofore ephemeral nature of quotidian activity” caused by the “overlapping web” of recorded memories that would stem from lifelog use that has become as common as the cell phone.⁸⁹ Their point may be that societies will adjust much as they have adjusted to the ubiquitous digital camera, video cameras and the chatting, chiming and distraction caused by mobile telephones and pdas—bugs don’t stop the picnic.⁹⁰

The Total Recall team predict and embrace the fact that lifelogging recordings would fall into the hands of the state. Indeed, part of their social design concept for

88 C. Cheng, L. Golubchik, and D.G. Kay, “Total Recall: Are Privacy Changes Inevitable?,” Proc. First ACM Workshop on Continuous Archival and Retrieval of Personal Experiences, ACM Press, 2004, pp. 86-92; <http://bourbon.usc.edu/iml/recall/papers/>.

89 .C. Cheng, L. Golubchik, and D.G. Kay, “Total Recall: Are Privacy Changes Inevitable?,” Proc. First ACM Workshop on Continuous Archival and Retrieval of Personal Experiences, ACM Press, 2004, pp. 86-92; <http://bourbon.usc.edu/iml/recall/papers/>.

90 But see Gaia Bernstein, *When Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 Villanova L. R. (2006) (Legal norms and technological protections of privacy may be inferior to aptly timed “social shaping” whereby privacy protecting practices and incentives are integrated into appropriate settings.) Cf. Scott Carlson, *On the Record, All the time*, 53 Chronicle of Higher Education (examining practical social issues posed by audio and video lifelogging).

lifelogs is that they are “available to the judicial system.” They note with seemingly uncritical acceptance that “the political climate supports access to information by law enforcement even without judicial intervention”. They speculate that Total Recall recordings would be admissible as veridical under the rules of evidence because of the “legitimate needs for data” and that they probably would not be subject to Fifth Amendment exclusion because they would not be “testimonial”. Rather than “degrade” the utility of the lifelog out of concerns about privacy and government access, the Total Recall team has labored to imagine designs features that acknowledge privacy interests in turning lifeloggers on, off and away, while insuring the capacity to preserve verifiably authentic, unmodified recordings. It is that very capacity, preserved at all, that constitutes the threat.

Conclusion

The ultimate dream of lifelogging is to create and preserve a complete and useable record of one’s own life. Andy Warhol got the Andy Warhol Museum, and a lot of other people would like to have the cyber equivalent. The point of a lifelog need not be social critique, self-aggrandizement or immortality, though. It could be entertainment, sharing, or improving health or personal insight. Yet, whatever the motives for lifelogging, creating such a record has troubling implications for privacy, moral repair, mental health, and ideal of limited government.⁹¹

91 Cf. Jed Rubenfeld, "The Right of Privacy," 102 Harvard Law Review 737 (1989) (defending a principle that individual rights should be ascribed to prevent government becoming totalitarian).

Comprehensive full-life lifelogging technology does not yet exist outside the laboratory and is not, therefore, ripe for legal rules and regulation. Yet ethical limitations and design parameters suggest themselves.⁹² No one should be required to keep a lifelog. No one should be suspected for not keeping a lifelog. Personal lifelogs should be deemed the property of the person or persons who create them. No one should record or photograph others for a lifelog without consent of the person or their legal guardian. A counter-technology to block lifelog surveillance should be designed and marketed along with lifeloggers. The owner/subject of a lifelog should be able to delete or add content at will. No one should copy a lifelog or transfer a lifelog to a third party without the consent of its owner.

We must hope that the changes in the quality of life affected by the proliferation of lifelogs will not result in a further deterioration in of the taste for privacy or fewer legal privacy protections. Existing privacy laws pertaining to intrusion, publication,

92 See generally, modified guidelines for proposals submitted to DARPA for its LifeLog project: “offerors must also address human subject approval, data privacy and security, copyright, and legal considerations that would affect the LifeLog development process.’ The purpose of this modification is to reiterate this requirement and to provide clarification guidance regarding the capture by LifeLog sensors of imagery and audio of people other than the user of the LifeLog system, and to extend the initial due date for proposals. LifeLog researchers shall obey all applicable privacy laws and regulations, and shall avoid even the appearance of the invasion of privacy. LifeLog physical data capture systems shall allow the LifeLog user to dynamically activate and deactivate the recording of audio and video, independent of data stream processing such as using optical flow or ambient light and noise to measure motion or transitions between indoors and outdoors. LifeLog researchers shall not capture imagery or audio of any person without that person's a priori express permission. In fact, it is desired that capture of imagery or audio of any person other than the user be avoided even if a priori permission is granted.”

communication, search and seizure, surveillance, data protection and identity should be presumed to apply to lifelogs. Existing intellectual property laws should be presumed to apply to lifelog content. These presumptions may prove unworkable or merely unpopular. For better or for worse, one must anticipate that the law will not create a special shroud of privacy for lifelogs. It is likely that lifelogs -- by analogy to functionally similar personal papers, recordings, data and communications-- will be subject to the legal rules of document creation, retention and destruction; litigation discovery; government search and seizure; government administrative subpoena; self-incrimination; privilege; and professional ethics. To encourage cautious, self-aware use, the legal risks of lifelogging should be emphasized by those who design, create and market the new technologies.