University of Pennsylvania Carey Law School
Penn Law: Legal Scholarship Repository

Faculty Scholarship at Penn Law

2008

Dredging Up the Past: Lifelogging, Memory and Surveillance

Anita L. Allen
University of Pennsylvania Carey Law School

Follow this and additional works at: https://scholarship.law.upenn.edu/faculty_scholarship

 Part of the Communication Technology and New Media Commons, Computer Law Commons, Constitutional Law Commons, Ethics and Political Philosophy Commons, Intellectual Property Law Commons, Jurisprudence Commons, Law and Society Commons, Privacy Law Commons, Public Law and Legal Theory Commons, Science and Technology Law Commons, and the Social Psychology Commons

Repository Citation

Allen, Anita L., "Dredging Up the Past: Lifelogging, Memory and Surveillance" (2008). *Faculty Scholarship at Penn Law*. 167.
https://scholarship.law.upenn.edu/faculty_scholarship/167

This Article is brought to you for free and open access by Penn Law: Legal Scholarship Repository. It has been accepted for inclusion in Faculty Scholarship at Penn Law by an authorized administrator of Penn Law: Legal Scholarship Repository. For more information, please contact PennlawIR@law.upenn.edu.

SYMPOSIUM

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 Gemmell[1]

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.

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

† Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania.

1 Alec Wilkinson, *Remember This? A Project to Record Everything We Do In Life*, New Yorker 38, 39 (May 28, 2007).

2 A New York Times–sponsored webpage lists the complete contents of the Westinghouse time capsule. See *1939 Westinghouse Time Capsule Complete List Contents*, NY Times Mag (1996), online at http://www.nytimes.com/specials/magazine3/items.html (visited Jan 12, 2008).

3 For a description of Andy Warhol's time capsule project, see *The Warhol: Collections/Archives* (The Andy Warhol Museum 2007), online at http://www.warhol.org/collections/archives.html (visited Jan 12, 2008):

> 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

File: 3 Allen Final 2.19 Created on: 2/19/2008 2:06:00 PM Last Printed: 2/19/2008 2:12:00 PM

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 died in 1987, leaving for the future a solipsistic collection of personal clutter. The Andy Warhol Museum in Pittsburgh 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.

Andy Warhol deliberately wove archiving into the fabric of his everyday life for years, allowing the happenstance of solitary and social experience to substantially 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 twentieth century time-capsuling and the technological conceit of twenty-first century "lifelogging."

I. LIFELOGGING

The term "lifelog" refers to a comprehensive archive of an individual's quotidian existence, created with the help of pervasive computing technologies: "A life-log 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]

> 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. For an account of contemporary views on Andy Warhol, see Robin Pogrebin, *A Portrait of an Artist Both Loved and Hated*, NY Times E1, E8 (Sept 20, 2006).

5 Martin Dodge and Rob Kitchin, *Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting*, 34 Envir & Planning B: Planning & Design 431, 431 (2007). See also Martin Dodge and Rob Kitchin, *The Ethics of Forgetting in an Age of Pervasive Computing* 1 (CASA Working Paper Series 92, Mar 2005), online at http://www.casa.ucl.ac.uk/working_papers/paper92.pdf (visited Jan 12, 2008) (characterizing lifelogs, among other things, as

Lifelog technologies would record and store everyday conversations, actions, and experiences of their users, enabling future 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 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 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 webpage 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"

"socio-spatial archives that document every action, every event, every conversation, and every material expression of an individual's life").

6 A Nokia product, Lifeblog, archives cell phone messages and photographs. See Mark Ward, *Log Your Life via Your Phone*, BBC News Online (2004), online at http://news.bbc.co.uk/2/hi/technology/3497596.stm (visited Jan 12, 2008). Weblog technology that enables users to record thoughts, photos, video, and audio is being marketed under the "lifelog" rubric. See, for example, Real Life Log, online at http://www.reallifelog.com (visited Jan 12, 2008).

7 See generally Dodge and Kitchin, 34 Envir & Planning B: Planning & Design 431 (cited in note 5).

8 University of Toronto professor Steve Mann has been a pioneer in the field of wearable computers, countersurveillance, and lifelogging. See Steve Mann, Personal Web Page, online at http://wearcam.org/steve.html (visited Jan 12, 2008); EyeTap Personal Imaging Lab (University of Toronto), online at http://www.eyetap.org/about_us/people/index.html (visited Jan 12, 2008). See also Frank Nack, *You Must Remember This*, 12 IEEE Multimedia 4, 5 (2005), online at http://www.eyetap.org/papers/docs/ieee_media.pdf (visited Jan 12, 2008) (comparing Mann's "Eye Tap" lifelogger, which alters the image of the world presented to the logger, to MyLifeBits).

9 See Wilkinson, *Remember This?*, New Yorker at 39 (cited in note 1), quoting Jim Gemmell. See also Gordon Bell and Jim Gemmell, *A Digital Life*, Scientific Am 58, 58–60 (Mar 2007) (tracing lifelogging from its origins in post-WWII technologies to the present and hypothesizing about future inroads lifelogging may make into daily lives).

10 Bell and Gemmell, *A Digital Life*, Scientific Am at 62 (cited in note 9).

11 Electronic media of storage raise problems of transience. Bell recognizes that parts of his archive could become unreadable one day. If the current compression standard for photos (.jpeg) were supplanted, for example, stored images would become inaccessible. See Wilkinson, *Remember This?*, New Yorker at 44 (cited in note 1).

lifeloggers. Lifelogging devices will be inexpensive in the future, too. Mr. Bell estimates that sixty 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 forgotten. Stricken with Alzheimer's Disease, Ronald Reagan likely forgot he had been President of the United States.[15] To address the problem of fallible memory, the ancients relied on mnemotechnology, storytelling, pictures, and, eventually uniform systems of writing.[16] Lifelog innovators are promising to better the ancients with their memory machines. The idea of a memory machine was once pure fantasy.[17] But technologists predict that full-life lifelogging devices will one day be integrated into everyday existence, becoming as ordinary as telephones.[18] 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 Southern California.[19] Total Recall re-

12 Clive Thompson, *A Head for Detail*, Fast Company 73, 77 (Nov 2006).

13 See generally Daniel L. Schacter, *The Seven Sins of Memory: How the Mind Forgets and Remembers* (Houghton Mifflin 2001) (classifying memory malfunctions into seven categories, based upon the malfunctions' relationships to otherwise positive neurological functions).

14 See, for example, H. Branch Coslett, *Consciousness and Attention*, 17 Seminars in Neurology 137, 137–39 (1997), in which a memory and brain disorder researcher describes the relationship between attention and consciousness.

15 See David Shenk, *"Does He Remember Being President?": The Downward Spiral of Ronald Reagan's Alzheimer's*, Beliefnet.com (2006), online at http://www.beliefnet.com/story/147/story_14713_1.html (visited Jan 12, 2008).

16 See, for example, Frances A. Yates, *The Art of Memory* 55 (Chicago 1966) (describing how ancient Greek and Roman authors developed a "mnemotechnology" of improving the ability to remember details of argument and perspective by associating ideas with visual, often architectural imagery).

17 See José Van Dijck, *From Shoe Box to Performative Agent: The Computer as a Personal Memory Machine*, 7 New Media and Socy 311, 314–16 (2005) (describing the "Memex" machine fantasy introduced in Vannevar Bush, *As We May Think*, Atlantic Monthly 101, 106 (July 1945)).

18 See Van Dijck, 7 New Media & Socy at 319–24 (cited in note 17) (describing Lifestreams, Memories for Life, and MyLifeBits visionary lifelog projects, all aimed at preserving life experiences in a seamless, invisible way that exploits digital technologies).

19 For a description of the Total Recall project at the University of Southern California, see University of Southern California Multimedia Lab, *Total Recall: A Personal Information Management System* (2005), online at http://bourbon.usc.edu/iml/recall (visited Jan 12, 2008):

searchers 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 our social structure."[20] They anticipate mostly positive changes and net benefits relating to education, law enforcement, health care, and sense and memory enhancement for the disabled.[21]

The Defense Advanced Research Projects Agency (DARPA) is the central research and development arm of the Department of Defense.[22] 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."[23] 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 imagery, audio, or video replay of the event."[24] 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.[25]

For generals, edgy artists, and sentimental grandmothers alike, lifelogging could someday replace or complement existing memory preservation practices. Like a traditional diary, journal, or daybook, the lifelog could preserve subjectively noteworthy facts and impres-

> 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 quality of life.

See also William Cheng, Leana Golubchik, and David Kay, *Total Recall: Are Privacy Changes Inevitable?*, Proceedings of the 1st ACM Workshop on Continuous Archival and Retrieval of Personal Experiences 86 (Oct 15, 2004) (proposing a complex encryption framework as a solution to privacy concerns in a lifelogging world).

20 Cheng, Golubchik, and Kay, *Total Recall* at 86 (cited in note 19). See also Thompson, *A Head for Detail*, Fast Company at 76–78 (cited in note 12) (reporting on Gordon Bell's lifelogging projects and suggesting that Bell's rituals may soon become mainstream).

21 Cheng, Golubchik, and Kay, *Total Recall* at 86 (cited in note 19).

22 For a general description of its mission, see DARPA's website, online at http://www.darpa.mil (visited Jan 12, 2008).

23 DARPA, *LifeLog Proposer Information Pamphlet*, SOL BAA 03-30 (2003), available online at http://web.archive.org/web/20030603173339/http%3a//www.darpa.mil/ipto/Solicitations/PIP_03-30.html (visited Jan 12, 2008).

24 Id.

25 DARPA abandoned its LifeLog project. See id. 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 Shane Harris, *Administration: TIA Lives On*, Natl J 66 (Feb 25, 2006).

File: 3 Allen Final 2.19 Created on: 2/19/2008 2:06:00 PM Last Printed: 2/19/2008 2:12:00 PM

sions. 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.

II. THE APPEAL OF THE LIFELOG

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's majestic humanism[26] and

---

[26] See generally Giovanni Pico Della Mirandola, *Oration on the Dignity of Man* (Henry Regnery 1956) (A. Robert Caponigri, trans).

> 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

Immanuel Kant's enlightened liberalism,[27] most of every human life is as fungible and forgettable as a mass-produced soup can.[28] Furthermore, the potential would be great for incivility, emotional blackmail, 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.

III. 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

> 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!

Pico Della Mirandola, *Oration on the Dignity of Man* (Wisconsin State University 1996) (Richard Hooker, trans), online at http://www.wsu.edu/~dee/REN/ORATION.HTM (visited Jan 12, 2008).

27 Immanuel Kant, *What Is Enlightenment?*, in Lewis White Beck, ed, *Foundations of the Metaphysics of Morals and What Is Enlightenment?* 85 (Liberal Arts 1959):

> 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.

28 I allude, of course, to Andy Warhol's famous canvases depicting Campbell's soup cans, which render a mundane generic object into something of interest. See generally *The Warhol: Resources and Lessons: Campbell's: Ode to Food* (The Andy Warhol Museum 2007), online at http://edu.warhol.org/aract_soup.html (visited Jan 12, 2008).

File: 3 Allen Final 2.19 Created on: 2/19/2008 2:06:00 PM Last Printed: 2/19/2008 2:12:00 PM

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"—"units of data that have been selected and harvested from the sum of potential data."[29] Because lifelog data is conceived as self-produced, Martin Dodge and Rob Kitchin have characterized lifelogging as personal "sousveillance."[30] Lifelogging has sousveillance and surveillance dimensions.[31] 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 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?[32] How can secu-

---

29 See Dodge and Kitchin, 34 Envir & Planning B: Planning & Design at 432 (cited in note 5).

30 Id at 434. They borrow the term "sousveillance" from Steve Mann. See id, citing Steve Mann, Jason Nolan, and Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 Surveillance and Socy 331, 332 (2003).

31 See Steve Mann, *Equiveillance: The Equilibrium between Sur-veillance and Sousveillance* 2 (On the Identity Trail, May 2005), online at http://www.idtrail.org/files/Mann,%20Equiveillance.pdf (visited Jan 12, 2008):

> 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.

32 See, for example, Philip Agre, *Surveillance and Capture: Two Models of Privacy*, 10 Info Socy 101, 105–07 (1994) (contrasting metaphorical understandings of privacy). A given person

rity 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.

IV. 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 five thousand years, like a World's Fair time capsule. By design, lifelog capta will be accessible and useable. Moreover, the act of capturing data itself implicates privacy concerns of all sorts, not just informational privacy and data protection.[33] 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.[34] 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

may or may not specifically intend "surveillance" and yet collect ("capture") data of the sort that would result from intentionally spying on others.

33 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* 3–6 (West 2007) (discussing the various meanings various speakers ascribe to the word "privacy"); Anita Allen, *Privacy*, in William G. Staples, ed, 2 *Encyclopedia of Privacy* 393 (Greenwood 2007).

34 DARPA modified its original call for proposals to acknowledge research ethics and other ethical, legal, and social implications. See DARPA, *LifeLog Modification 3*, SOL BAA 03-30 (2004), available online at http://web.archive.org/web/20030621133355/www.darpa.mil/ipto/solicitations/Mod3_03-30.html (visited Jan 12, 2008):

> 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.

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.

A. Pernicious Memory

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.[35] 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 getup, 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 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 the practical utility suggested by the foregoing illustrations, electronic memory enhancement is not an unqualified good. Electronic memory enhancement enables destructive reminding and

---

35 See, for example, 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.").

remembrance. The unredacted lifelog could turn into a bigger burden on balance than fallible biological memory *cum* conventional contemporary enhancements.

1. 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. Worldwide 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.[36] In order to create that distance, they need to be safe from memory: they need to forget and need others to forget, too.[37]

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.[38]

Melvin v Reid[39] pitted a homemaker, who had once been a prostitute wrongly accused of murder, against filmmakers who used her ac-

36 Uncommon errors such as perpetrating large-scale human rights atrocities are another matter. Adolf Hitler likely had no moral interest in distancing himself from his role in the Holocaust.

37 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.

38 The "dredging up the past" cases I have in mind date back to the 1930s. See text accompanying notes 39–42. Some of the more recent cases in the line include *Willan v Columbia County*, 280 F3d 1160, 1163 (7th Cir 2002) (finding no liability where police queried computerized database maintained by the FBI's National Crime Information Center and discovered that a mayoral candidate had been convicted of felony burglary in 1980's in another state); *Uranga v Federated Publications*, 67 P3d 29, 35 (Idaho 2003) (finding no liability for republication of a forty-year-old court record associating the plaintiff with homosexuality); *Hall v Post*, 372 SE2d 711, 717 (NC 1988) (finding no liability for publishing story about a woman who many years earlier had been married to a carnival barker and abandoned their child).

39 297 P 91 (Cal Ct App 1931).

tual maiden name in *The Red Kimono*, a movie based on her life.[40] The *Melvin* court held that the policy interest of the state in rehabilitation justified allowing the woman's privacy suit to stand.[41] 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.[42] Mr. Sidis had been a celebrated child 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 Association*,[43] was brought by a convicted armed hijacker turned solid citizen and parent who sued a newspaper for publishing a reference to his crime.[44] 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—or as 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

---

40 Id at 93:

> 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.

41 But see *Willan*, 280 F3d at 1162 ("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."). The Supreme Court held in *Cox Broadcasting Corp v Cohn*, 420 US 469 (1975), 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.)

42 See *Sidis v F-R Publishing Corp*, 113 F2d 806 (2d Cir 1940). In *Sidis*, the court noted that *The New Yorker* article about the former prodigy was "merciless" and "ruthless," but concluded that

> [r]egrettably or not, the misfortunes and frailties of neighbors and "public figures" are subjects of considerable interest and discussion to the rest of the population. And 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.

Id at 809.

43 483 P2d 34 (Cal 1971), overruled by *Gates v Discovery Communications, Inc*, 101 P3d 552 (Cal 2004) (holding that a corporation was not liable to an offender for publishing facts obtained from public official records).

44 *Briscoe*, 483 P2d at 542 ("A jury might well find that a continuing threat that the rehabilitated offender's old identity will be resurrected by the media is counter-productive to the goals of [rehabilitation].").

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.[45] The crucial inquiry is whether judges and juries examining the facts would be likely to find that a lifelog data disclosure was "highly offensive to a reasonable person" and not newsworthy or otherwise of "legitimate interest to the public."[46]

It is conceivable 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 (for example, 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 US law to discount the significance of privacy in public.[47]

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

---

45 North Carolina rejected the private fact tort in *Hall*, 372 SE2d at 717:

> 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.

46 See Restatement (Second) of Torts § 652B (1977):

> 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.

See also id § 652D(a)–(b):

> 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.

47 See Anita L. Allen, *Uneasy Access* 125–28 (Rowman & Littlefield 1988) (noting courts' general unwillingness to recognize any broad right to privacy in public). See also Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L & Philosophy 559, 573–75 (1998) (citing examples of courts' reluctance to allow one person's privacy rights to encroach on the freedom of others).

rights, knowingly wounding people who are trying to forget their pasts.[48] 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. It would have taken some dredging to uncover it. Hence the plaintiffs developed expectations of privacy and secrecy, around which they built their interpersonal relationships. This was especially true of the plaintiffs in *Briscoe* and *Melvin*, neither of whom had ever experienced national celebrity. Sidis had been a 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."[49] *The New Yorker* violated "norms of appropriateness" by using deception to gain fresh access to Sidis, and norms of fair informa-

---

48 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 Society of Professional Journalists, *Code of Ethics* (1996), online at http://www.spj.org/ethicscode.asp (visited Jan 12, 2008):

> 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.

See also Anita L. Allen, *Why Journalists Can't Protect Privacy*, in Craig LaMay, ed, *Journalism and the Debate over Privacy* 69 (Lawrence Erlbaum 2003) (observing the demise of the privacy-protection norms among practicing journalists and explaining the practical limits on privacy protection).

49 See Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U Chi L Rev 919, 988 (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.").

tion "distribution" when it republished facts about Sidis younger people did not know and most older people had forgotten.[50]

2. 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 memory and mostly paper archives was an obligation that ethical principles of care and character would surely dictate.[51]

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[52] (FOIA's) privacy exemptions to protect individuals from the federal government releasing their criminal "rap sheets" to the media.[53] Criminal histories are public data, the court argued, but data that ordinarily enjoys "practical obscurity."[54] Thus "[t]he privacy interest in maintaining the practical obscurity of rap-sheet information will always be high."[55]

In an era of electronic archives, traditional predictions and expectations of privacy about the past have begun to look less reasonable.

---

50 Compare Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash L Rev 119, 136 (2004) (distinguishing norms of appropriateness and distribution norms for information disclosures).

51 But see H.J. McCloskey, *The Political Ideal of Privacy*, 21 Phil Q 303, 308–09 (1971). 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.

52 Pub L No 89-554, 80 Stat 383 (1966), codified as amended at 5 USC § 552 (2000 & Supp 2002).

53 *DOJ v Reporters Committee for Freedom of the Press*, 489 US 749, 771 (1989):

> 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. . . . [FOIA] Exemption 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."

54 Id at 780.

55 Id:

> 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.

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 1980s in another state.[56] 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 databases 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 government records, but in videos, telephones, weblogs, Twitter, Facebook, and MySpace, as well. Whole television programs are based on videos of crimes being committed—robberies, shootings, high-speed chases, sexual predation, and criminal solicitation.[57] The 2007 Virginia Tech campus massacre[58] was documented in video and audio recordings made by Swedish exchange students, wounded victims, and by the suicidal murderer himself.[59] These recordings 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.

---

56 See *Willan*, 280 F3d at 1163.

57 See generally Deborah Jermyn, *Crime Watching: Investigating Real Crime TV* (I.B. Tauris 2007).

58 Alessandra Stanley, *Deadly Rampage and No Loss for Words*, NY Times A19 (Apr 17, 2007).

59 See Howard Kurtz and Soledad O'Brien, *The Massacre at Virginia Tech—Part 2*, CNN (Apr 22, 2007).

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 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.[60] 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.[61] But videotaping is less stringently regulated, and videotaping in public places, short of upskirting, harassment, or stalking, is rarely unlawful.[62]

Lifelogs will be downplayed by some technology enthusiasts as an incremental rather than 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.

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 policymakers 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.

---

60 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 Cheng, Golubchik, and Kay, *Total Recall* at 88 (cited in note 19).

61 See, for example, *Moore v Telfon Communications*, 589 F2d 959, 965–66 (9th Cir 1978) (interpreting the federal wiretap act as prohibiting nonconsensual recording of telephone calls but permitting recordings that preserve evidence of a crime).

62 See, for example, *United States v Torres*, 751 F2d 875, 884–86 (7th Cir 1984) (holding that, while videotaping is not governed by the federal wiretap laws, Fourth Amendment considerations may still apply).

B. 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.[63] The lifelogging concept is insensitive to the therapeutic value of forgetting the details of experience.[64] 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.[65] 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.

Another psychological hazard is harder to fix: voluntary, but pathological rumination.[66] The technology will enable excessive rumination

---

63 See, for example, Marc Augé, *Oblivion* 17 (Minnesota 2004) (Marjolijn de Jager, trans) ("One must know how to forget in order to taste the full favor of the present, of the moment, and of expectation.").

64 See Jeanie Lerche Davis, *Forget Something? We Wish We Could*, WebMd (Apr 9, 2004), online at http://www.webmd.com/anxiety-panic/features/forget-something-we-wish-we-could (visited Jan 12, 2008).

65 See, for example, Adam J. Kolber, *Therapeutic Forgetting: The Legal and Ethical Implications of Memory Dampening*, 59 Vand L Rev 1561, 1595–98 (2006) (arguing that 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).

66 Ellen McGrath, *The Rumination Rut*, Psych Today (Apr 11, 2003), online at http://psychologytoday.com/articles/pto-2687.html (visited Jan 12, 2008). See also Michael E. Addis and Kelly M. Carpenter, *Why, Why, Why?: Reason-giving and Rumination as Predictors of Response to Activation- and Insight-oriented Treatment Rationales*, 55 J Clinical Psych 881, 882–84 (1999) (analyzing the connection between a patient's explanation for his depression and the most effective treatment for that patient).

by persons experiencing unipolar or bipolar depression.[67] 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 capta are not fixed, "hard" evidence of an important whole story, but 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.[68] But how useful is forgiveness when there is a diminished capacity to forget?

Indeed, the ability to move on from wrongdoing 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. Deleting data about my forgiven offenses from 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 about wrongs will not be consistently followed up with information about moral repair. Another difficulty is 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 secret lifelog data of forgivable forgiven wrongs.

C. 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 about individuals is already collected and retained, some by the individual, some by others. In the future the need

---

67 A person predisposed to ruminate may do so excessively whether her memory bank is vast or nearly vacant. See Addis and Carpenter, 55 J Clinical Psych at 883 (cited in note 66). My speculation is that a culture of memory machines may exacerbate problems of pathological rumination.

68 See, for example, Kay Redfield Jamison, *An Unquiet Mind* 120–22 (Knopf 1995), in which a bipolar professor of psychiatry describes the violence, remorse, and forgiveness precipitated by her own mental illness.

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 lifelog data featuring the conduct of others. The potential thus exists for using lifelog pervasive computing technology for purposes of spying on others.[69] 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.[70] 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, to the extent possible, continue to act with respect for the moral autonomy and for the moral and legal interests of the investigative target.[71] This value attached to spying thus provides no justification or defense for recreational spying, whether using lifelog 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

---

69 See, for example, Jeffrey A. Lowe, *Big Brother Will Be Watching: Lifelog Project Up Administration's Sleeve Threatens Privacy Rights of Every American*, LA Daily J 6 (July 31, 2003).

70 Anita L. Allen, *The Virtuous Spy*, 91 Monist (forthcoming 2008), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1010949#PaperDownload (visited Jan 12, 2008).

71 Id.

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,[72] 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.[73] Federal law and policy affirm the concept of search and seizure based on warrants and individualized suspicion, while allowing numerous exceptions in Fourth Amendment law, such as the "special needs" exceptions.[74] Although the Electronic Communications Privacy Act[75] enhances Fourth Amendment protections, it regulates government access to communications, stored data, and communications transactions records without barring access.[76] The Foreign Intelligence Surveillance Act[77] also regulates rather than prohibits access to premises, tangible items, and communications.[78] 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.[79]

---

72 See, for example, *People v Miller*, 60 Cal App 3d 849, 855 (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."). See also *Andresen v Maryland*, 427 US 463, 465 (1976) (holding that business records properly seized could be admitted into evidence without violating the "Fifth Amendment's command that '[n]o person . . . shall be compelled in any criminal case to be a witness against himself'"); *United States v Dawson*, 516 F2d 796, 807 (9th Cir 1975) (holding that the admission of a properly seized note from the defendant prisoner to another prisoner did not violate the defendant's protection against self-incrimination); *United States v Bennett*, 409 F2d 888, 897 (2d Cir 1969) (holding that a letter found during a lawful search, even though it was self-incriminating, could be admitted into evidence); *People v Thayer*, 408 P2d 108, 110 (Cal 1965) (noting that self-incriminating writings can be seized and admitted into evidence).

73 See *Whalen v Roe*, 429 US 589, 599–600 (1977) ("The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."). Several courts of appeals have validated *Whalen*'s informational privacy right. Helen L. Gilbert, Comment, *Minors' Constitutional Right to Informational Privacy*, 74 U Chi L Rev 1375, 1381–88 (2007).

74 See, for example, *Samson v California*, 547 US 843 (2006) (holding that the Fourth Amendment permits the search of a parolee without a warrant).

75 Electronic Communications Privacy Act of 1986, Pub L No 99-508, 100 Stat 1848.

76 See id.

77 Foreign Intelligence Surveillance Act of 1978, Pub L No 95-511, 92 Stat 1783, codified as amended at 50 USCA § 1801 et seq (2007).

78 See id.

79 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 FBI, *Press Release on National Security Letters*, online at http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm (visited Jan 12, 2008):

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 Chip concept of government access to encrypted data.[80] Yet, federal policy reflects the notion that new communications technology design must allow for government access and surveillance. This is the spirit of CALEA, the Communications Assistance for Law Enforcement Act.[81] CALEA compels the private sector to insure that new communications technologies do not thwart

---

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.

80 President Bill Clinton's White House announced the Clipper Chip Program in 1993. See White House Office of the Press Secretary, *White House Clipper Statement* (Apr 16, 1993), online at http://www.epic.org/crypto/clipper/white_house_statement_4_93.html (visited Jan 12, 2008). For a description of the Clipper Chip, see Electronic Privacy Information Center, *The Clipper Chip* (2001), online at http://www.epic.org/crypto/clipper (visited Jan 12, 2008):

> 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.

81 Communications Assistance for Law Enforcement Act, Pub L No 103-404, 108 Stat 4279 (1994). See also FCC, *Communications Assistance for Law Enforcement Act (CALEA)* (2007), online at http://www.fcc.gov/calea (visited Jan 12, 2008):

> 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.

law enforcement and its reach was recently extended to govern aspects of voice over internet protocol technologies.[82] While data destruction is a command of at least one federal privacy statute,[83] the federal government has sought to discourage automatic destruction of its own administrative records.[84] The government has moved against

---

82 See Second Report and Order and Memorandum Opinion and Order, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, No 04-295, *2 (May 3, 2006), online at http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf (visited Jan 12, 2008).

83 Video Privacy Protection Act of 1988 § 2(a)(2), Pub L No 100-618, 102 Stat 3195, codified at 18 USC § 2710(e) (2000):

> (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.

84 The federal government has complex record creation, disposal, and preservation guidelines. See National Archives, *Frequently Asked Questions about Records Management in General* (2001), online at http://www.archives.gov/records-mgmt/faqs/general.html (visited Jan 12, 2008). See, for example, Sue Dill Calloway, *Record Retention Periods*, HIPAAdvisory.com (2000), online at http://www.hipaadvisory.com/regs/recordretention.htm (visited Jan 12, 2008) (summarizing the federal document retention rules that are applicable to the private sector):

> 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 radipaharmaceutics 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.

the destruction of library[85] and ISP records.[86] The trend in Europe favoring mandatory private sector data retention is unlikely to remain on sister shores.[87]

- 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:
  1. Institutions receiving grants for research projects (52.8),
  2. 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
  3. 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).

[85] See American Library Association, *FBI in Your Library* (2007), online at http://www.ala.org/ala/oif/ifissues/fbiyourlibrary.htm#news (visited Jan 12, 2008) (discussing government efforts to obtain access to library records, bookstores, and internet trials).

[86] See James Plummer, *"Data Retention": Costly Outsourced Surveillance*, TechKnowledge Issue No 99 (Cato Institute Jan 22, 2007), online at http://www.cato.org/tech/tk/070122-tk.html (visited Jan 12, 2008):

> 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 Octo-

D. 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."[88] The developers of MyLifeBits have also broached this possibility, to reduce the attractiveness of lifelogs to the government.[89]

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."[90] They embrace a modified conception of lifelogs. The lifelogs 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' lifelogs, 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" the recording of some details, "forget" details over time, and "tweak" memory of the past by misrecording precisely when, where, and how

---

> ber. 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 Peter Fleischer and Nicole Wong, *Taking Steps to Further Improve Our Privacy Practices*, The Official Google Blog (Mar 14, 2007), online at http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html (visited Jan 12, 2008):

> 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.

87 On March 15, 2006 the European Union adopted Council Directive 2006/24/EC, 105 Off J Eur Communities 54, 54, 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). See id at 57 ("The obligation to retain data . . . shall include the retention of the data . . . relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services.").

88 See Dodge and Kitchin, 34 Envir & Planning B: Planning & Design at 442 (cited in note 5).

89 Wilkinson, *Remember This?*, New Yorker at 38 (cited in note 1).

90 Dodge and Kitchin, 34 Envir & Planning B: Planning & Design at 435 (cited in note 5).

certain events took place.[91] Fallibility of the lifelog will benefit the individuals who own it, too. Free from an "unforgiving" and "merciless" memory machine, persons are able to "evolve their social identities, to live with their conscience, to deal with 'their demons', to move on from their past to build new lives, to reconcile their own paradoxes and contradictions, and to be part of society."[92] 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 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 not be. 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."[93] They recognize the privacy issues raised by 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."[94] 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

91 Id at 441.

92 Id at 443.

93 Cheng, Golubchik, and Kay, *Total Recall* at 87 (cited in note 19).

94 Id.

web" of recorded memories that would stem from lifelog use that has become as common as the cell phone.[95] Their point may be that societies will adjust much as they have adjusted to the ubiquitous digital cameras, video cameras, and the chatting, chiming, and distraction caused by mobile telephones and PDAs—bugs don't stop the picnic.[96]

The Total Recall team predicts and embraces the fact that lifelogging recordings will fall into the hands of the state. Indeed, part of their social design concept for lifelogs is that they are "available to the judicial system."[97] They note with seemingly uncritical acceptance that "the political climate supports access to information by law enforcement even without judicial intervention."[98] They speculate that Total Recall recordings will be admissible as veridical under the rules of evidence because of the "legitimate needs for the data" and that they probably would not be subject to Fifth Amendment exclusion because they would not be "testimonial."[99] Rather than "degrade" the utility of the lifelog out of concerns about privacy and government access, the Total Recall team has labored to imagine design 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 his museum, and many other people would like to have the cyber equivalent. The point of a lifelog need not be social critique, self-aggrandizement, or immortality. 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 the ideal of limited government.[100]

---

95 Id.

96 See, for example, Scott Carlson, *On the Record, All the Time*, Chronicle of Higher Education A31, A33–35 (Feb 9, 2007) (examining practical social issues posed by audio and video lifelogging). But see generally Gaia Bernstein, *When Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 Vill L Rev 921 (2006) (remarking that 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.).

97 Cheng, Golubchik, and Kay, *Total Recall* at 88 (cited in note 19).

98 Id.

99 Id.

100 See, for example, Jed Rubenfeld, *The Right of Privacy*, 102 Harv L Rev 737, 784–85 (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.[101] 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 the consent of the person or their legal guardian. A countertechnology 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 of the taste for privacy or fewer legal privacy protections. Existing privacy laws pertaining to intrusion, publication, 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.

101 See generally DARPA, *LifeLog Modification 3* (cited in note 34).