Privacy 2015

Michael E. Buerger

Few of our fundamental concepts are under greater pressure than that of privacy. It is challenged overtly in the name of national security by the provisions of the USA Patriot Act, and covertly by the unexplained and unexamined small print of commerce. It is challenged not only by technical engineering, but also by the social engineering that has arisen from enhanced technological capacities. The questions of whether privacy as we currently understand it will still exist in 2015 seems to lie in the balance in 2005.

In American law, legal concepts of privacy derive not from explicit articulation, but from "penumbras" of other principles and words within the Constitution and the Bill of Rights. Those documents were written in an era when the world of physical space constituted the entire known universe. When the Fourteenth Amendment was written, long-distance communications were the province of Samuel Morse's telegraph, and age-old technologies of drumbeats, smoke, and physical transportation of written messages. The modern emergence of cyberspace has created a virtual new world in which space and time are compressed, altering the fundamental rules by which we have lived. Chief among those changes, cyberspace has bestowed upon almost all of us a parallel identity that is virtually limitless, disconnected from our physical "real" selves, and in important ways not under our control.

It is not so much that cyberspace created new problems, because the privacy and identity problems that plague us today have analogs in the physical world. Rather, the speed and scale of information transmission in the Information Age exacerbates those problems, substantively transforming them, magnifying their power, and perhaps creating something fundamentally different from their historical cousins.

Our notions of privacy are anchored in the concrete, physical world of agrarian England, ghosts of a world long gone. Thomas Cowper (in this volume) rightly speaks of our understanding of information as an artifact of the Industrial Age, but the accelerated change of technology is asynchronous with the social developments that use, constrain, retard, or banish technology. The modern age is a battleground in that sense, between shifting alliances of forces that alternately embrace or renounce technological advances according to principles and desires that are disconnected from the technology itself. The challenge presented by the onslaught of technology is whether it will be a master or a tool; the current interrelated debates over the extent of privacy similarly inquire whether a concept so anciently conceived can long endure.

Personal, Private, and Public

Whether "a reasonable expectation of privacy" survives to 2015 in any form depends upon the arc of developments in three main areas:

1) the personal decisions of individuals to surrender their expectations of privacy voluntarily, or haphazardly, in search of some thing or things deemed valuable to them;
2) government restrictions placed upon private sector use of data in the interests of a recognized "common good"; and
3) legal restrictions upon government's use of data and technology.

It is possible that "a reasonable expectation of privacy" is a frog, slowly being boiled without understanding what is happening to it. As technological advances becomes so pervasive, and the economy so dependent upon credit, the law

finally may bow to the commonplace reality and no longer require obeisance to an archaic 18th century notion. The alternative possibility is that real and perceived abuses will mobilize the citizenry to take steps to reassert the centrality of "the right to be left alone," not only by the forces of government, but also by the titans of industry and finance.

A central question in the debate will be whether my individual control over the multiple ethereal abstract renditions of "myself" that exists in the databases constitutes a fundamental right. If it is, a host of regulatory actions may be taken by government. If it is not, we enter into a brave new world with fundamentally different expectations of the nature of society and social interaction.

Expectations and Limits

Advocates of greater information-seeking tools consistently remind us that privacy is not synonymous with anonymity, and that anonymity is neither a right nor a reasonable expectation. That remains true, but was also true in the physically defined world. None of us are invisible, able to pass through public space without being observed. Few of us maintain solitary lives "off the grid," though many live with relative anonymity in the turbulent flow of humanity in the cities.

Physical protections of privacy could be overcome—conversations could be overheard; non-verbal actions, reactions, and signals observed; written communications read over the shoulder--but with some balance. Physical proximity was required to eavesdrop, and with proximity came the counter-threat of exposure, alerting the target to the surveillance, and allowing countermeasures (including silence, deferring communication to another time and place, the use of codes, etc.). As communications expanded over longer distances by telegraph, telephone, and radio transmitter, more surreptitious interceptions became possible. Security depended upon codes, and luck. (The use of the Navajo language by the Code Talkers in World War II stands out as a prime example of successful code protection, but it rested upon the physical and social isolation of the Navajo Nation from the Japanese. Whether a similar scheme could be as successful today is perhaps more problematic).

Several things have changed in the balance with our newest technologies, but three stand out. First is the permanence of the information—or, perhaps viewed from a different perspective, "the abstract representation of the individual, bound in time"—obtained, and its imperviousness to outside challenge. Second is the ability of the information-seeker to acquire and use the information in stealth. The third and perhaps most important area of concern is the susceptibility of the information to be used or altered without the knowledge of the individual it represents. A fourth problematic change looms in the background: the possibility that those who use the technology to seek exposure rather than privacy—the bloggers and exhibitionists—will somehow alter the terms of the debate, to the point where social expectations are of transparency rather than privacy.

(1) Permanence and Imperviousness

Our embarrassing and inglorious moments have always been observable to others (indeed, that visibility is usually the source of the embarrassment). In the physical world, they are largely confined to memory, and recede over time in both clarity and importance. While our temporary loss of dignity could be shared with others, it was largely a pale version, relayed verbally (with or without embellishments, to be sure), and a moment in time. The retelling could even work to our benefit, if the teller of tales was regarded as a gossip: distortion might be presumed by the audience,

diminishing the credibility of the report regardless of its accuracy. The observation that "your friends will know what's true and your enemies will assume what they want" could operate with relative ease. Even in cases where our lapses were known to be true, they constituted but one moment in our long association with friends and neighbors. Visual representation changes that dynamic, whether captured by closed-circuit surveillance cameras, a voyeur's hidden camera, or cell phone cameras of friends and associates.

Non-visual representations of self have been likewise transformed. If I had trouble paying my bills at one point in my life, in the immediate world my friends, associates, and neighbors know and remember it, but are also aware of my more recent history of fiscal responsibility. Their judgments of whether I am worthy of their trust will be based upon the totality of circumstances, presumably with the more recent given greater weight on the basis that they are more representative of my current abilities and disposition. In the new world of cyberspace, there exists no grace period in which to correct errors, no chance of recovery, and no redemption: our ghostly selves may drag Marley's chains with them forever.

Proponents of the wider use of technology point to a small group of incidents in which the unflinching eye of surveillance cameras helped resolve a case. From the Bulger case in London to the abduction of Carlie Brucia in Florida, televised images have aided in the solving of crimes. Opponents point to the less certain impact of CCTV on crime prevention, and to the early failures of biometric scanning at public events (Reuters 2003). They question not only the difference between the social cultures of the United Kingdom (where CCTV is widely used and widely accepted) and the United States (where CCTV in public spaces is still a relatively rare phenomenon, and less widely acclaimed), but the deterrent effect itself, citing numerous individuals who rob convenience stores and banks, despite the obvious presence of security cameras. The Beltway "cell phone bandit" is but the latest and most intriguing of a long line of rievers who are either oblivious to or contemptuous of the technology set up to deter or ensnare them.

(2) Stealth Acquisition

In one respect, "privacy" is less the issue than security. In order to participate in modern life, we have little choice but to part with a certain amount of information about ourselves. To obtain credit, we must demonstrate that we are worthy of it, that we have a history of paying our debts, that we have assets commensurate with the risk we ask the lender to take with us. To obtain and use health benefits, and insurance, we have to divulge certain information about our habits and conditions so that we may swim in the appropriate part of the actuarial pool. In all of these endeavors, we are supplicants: we ask a larger polity for goods, services, and benefits beyond our individual ability to obtain. Most of us enter into those communal arrangements willingly, and with a tacit belief that the surrender of information is done in confidence, a dyadic relationship between ourselves and the service provider.

Technology altered the ground upon which we stood. When record keeping passed from paper files to electronic databases, the ease with which information could be shared expanded exponentially, and the cost dropped dramatically. In a nearly Orwellian transformation, things that were not forbidden suddenly became things that were permitted. Nothing existed that said personal information could not be shared, and so it was shared. Entire industries sprang up to sell information to other industries for marketing, and for other purposes masquerading as "research." In

the absence of legislation or regulation requiring that we be contacted when our supposedly confidential information was sought by others, the acquisition of wholesale batches of information became routine, subterranean, and profitable.

Technology also opened the way to another form of stealth acquisition: theft by hacking. The relatively open systems of commerce, with their relatively simple attempts at security, became the sneak thief's playground. The year 2005 brought news of multiple breaches of supposedly secure databases, and the loss or compromise of important information from ChoicePoint, Wells Fargo, the United States Air Force, several universities, and many supposedly protected sources.

(3) Transmogrification: Alteration and Suborning.

When a surreptitious video of public behavior can be easily made and posted to the Internet, that behavior is enshrined to an unintended, perhaps undeserving audience. If the video is edited and transformed into something it is not by compressing two separate actions into a single sequence (the act of picking one's nose, spliced onto the act of eating some popcorn, both occurring at separate times in a sports arena seat, for instance), a visual slander has been created. While the example here is relatively mild (it is an actual event, with crudely obvious splicing, viewed on a colleague's computer some years ago), the potential for greater trespasses is clear. "Seeing is believing" has first claim on a viewer's allegiance; its corollary, "believing is seeing," is often consigned to the dimly lit background.

While there is a question of whether or not we can be "harmed" if such an image is viewed by countless persons we will never meet in real life, nevertheless a fundamental shift has taken place. The amount of exposure to ridicule for everyday actions and conditions—once the sole realm of public figures and their paparazzi—has been foisted upon those who never sought to be public figures. The level of discomfort is only slightly lessened by relative anonymity: the threat of being accosted in a public setting by a cry of "Omigawd, it's the Booger-Eater!" lurks at the periphery of our vision.

Once upon a time, the closest we came to earthly immortality was to be on a mailing list. Those primitive databases seemed to last forever, oblivious to the passage of time…the inverse of fading human memory. On the Internet, they are not only timeless but replicatable, alterable. The most dramatic depiction of the potential for mayhem is the Sandra Bullock film *The Net*, now somewhat dated and a shade too Hollywood, but still a reasonable demonstration of the potential for mischief. At the core of the movie is the premise that the electronic representation of one's self is far more readily accepted in modern life than the corporeal self: the individual is dependent upon testimonial verification by their electronic *döppelgangers.*

Identity theft is easier than identity replacement, but even simple pranks and dirty tricks can cause mayhem. Hacking into online sex offender registries to delete records would have bad enough consequences. Were a malefactor to hack into one or more to create a false record bearing your information would be catastrophic (the basic premise of *The Net*). There are multiple means by which the slander could be verified as false, but almost all of them would come into play only after you were falsely and publicly branded as a pervert, a terrorist, a fellow traveler. As victims of even the simple financial identity theft have testified, the process of setting matters right again is tedious, lengthy, and painful.

Behind the notion of a "record" lies a need for some permanence of knowledge, a standard against which new information can be tested. Also implied in that permanence is the concept of

importance. From the first development of cylinder seals and cuneiform pictograms on clay tablets, commerce has depended upon records. Notations of births, marriages, and deaths written into family Bibles establish the linear descent of a clan, and the important linkages to others through marriage. The concept of sacred scriptures themselves—words so important they must be preserved forever, to inform exactly each new generation—epitomizes the deeply human need for a vehicle that conveys Truth (and its secular cousin, truth) across time and distance.

From clay tablets to data packets, economic and social stability has rested upon the foundation of a permanent record against which disputes could be tested. As the certainty of the records erodes under conditions of rapid proliferation, unverified augmentation, and potential distortion, there may be collateral losses in several spheres. A decline in consumer confidence may result in a constriction of the economy. To date, we have been concerned primarily with individual identity theft; if a second-stage corporate identity theft wave develops, it could affect capital projects, mergers, and the stability of trade. Unauthorized transfer of assets to offshore accounts, blocking of legitimate transfers to obstruct a purchase or payment, overwriting e-mail records with bogus "evidence" of wrongdoing and other forms of attack all undermine the foundations of legitimate commerce.

Unlike individual identity theft, we can predict that the resources to combat corporate theft will be considerable, and brought to bear in short order. Nevertheless, the impact of one incident will have ripple effects far beyond whatever damage is inflicted. As soon as the first case of corporate e-spionage takes place and becomes public knowledge, all corporate systems are both fair game, and suspect. E-spionage of the above-described sort may have occurred already, and kept behind the veil of proprietary information. The hacking arts embrace the ability to part that veil, however, and greater scrutiny of corporate records may result from both the Enron/WorldCom class of scandals and from the data mining brought to bear in the wars against terror and drugs.

The current line of forward thinking on such matters posits that "transparency" is the only reasonable defense against the suborning and misapplication of data. While that yet may be the case in some utopian future, in this particular arena the dictum that "the future is here; it is just not equally distributed" is most acute. Transparency cannot work for the individual unless corporate decision-making is equally transparent, and that is unlikely to happen in the near future. Government transparency is equally unlikely, even if some inroads are made into the present levels of over-classification of information. Secrecy acts against transparency as a form of Gresham's Law: as long as there are some secrets, there is no transparency, only selective exposure.

(4) Evolving Social Expectations

Beyond the international debate over ICANN and Internet copyrights is a second level of the question, "who controls the Internet?" Those who value privacy are invisible on the 'Net if they wish to be: until the day that money disappears, and all financial transactions are electronic, "protected" by biometric security measures, use of the Internet and the World Wide Web is voluntary. That may change by 2015, if the future is linear and driven solely by technological engineering, and Internet transactions become compulsory because they are the only game in town (outside the inevitable black markets that would develop). Social engineering remains a powerful force, however, and the disappearance of a cash economy is not a given.

The concurrent debate over illegal immigration and day labor, for instance, exists in

part because payments to migrants are (or can be) made in cash. Similar gray-market arrangements exist in childcare, elder care, automobile repairs and home improvements, among others, because smaller amounts of cash are essentially untraceable. If a combination of homeland security and taxation issues combine to eliminate paper money (which then would finally and literally be "not worth a Continental") in favor of traceable electronic transfers, we should anticipate a huge social dislocation of labor. The change will affect the undocumented and the non-documenting alike, and will have reverberations probably far beyond those of Sarbanes-Oxley.

The public face of the 'Net is those who use it for exposure, through blogging and webcasts (and the most recent innovation, podcasting). In a reversal of the "most embarrassing moments" material above, the Internet seems to thrive on them. Television had already staked out the ground, of course—from the old "Queen For A Day" show to the hapless and hopeless on "American Idol" and "The Apprentice"—but the 'Net widens Amateur Night astronomically. The bizarre celebrity of the Numa Numa dance (Feuer and George, 2005) may temporarily shame the protagonist, but perversely inspires imitators. Blogging does not just give voice to the closet Einsteins and Jeffersons and Hunter Thompsons of the age; it also provides a forum for the wildest opinions of every village idiot and drunken sot who can keep it together long enough to string words together on the keyboard. Indeed, with current estimates of 30% of Web traffic being sex-related, and a considerable underground developing for all sorts of antigovernment types (from the radical right of America's Christian Identity splinter groups to the democratic forces within China to the postings of al-Qaeda and the Taliban), there is a danger of a Gresham's Law here, as well. Codes of conduct may not be sufficient to curb the tendency to the lowest common denominator: outlaws scoff at codes, and only heed them when effective enforcement is imminent.

It is not bad enough to be expected to have a web page; everyone can also be Googled. While that is little more than what was possible with paper-driven systems, the ease and speed of the Internet search engines create an easy exposure that can be exploited by persons who wish us ill. The problem of stalkers using open records to locate their victims has already been widely published; the potential for similar exploitation by kidnappers, terrorists, political assassins remains thankfully unexploited, but a problem nevertheless. A comparable problem for law enforcement officers centers on the availability of their home addresses in online property records files. While many jurisdictions have enacted a patchwork of laws to fill these gaps, their mere existence gives the lie to the notion that protection lies in transparency. At best, transparency provides only limited protection against certain kinds of predations; it creates huge vulnerabilities to others.

This undercuts the premise of those who argue that privacy is dead, and transparency is the only effective defense against the misuse of data. The problem lies in the fact that transparency is like pregnancy—the system cannot be just partly transparent. Neither can one be constantly vigilant, at least not against attacks that can originate in any area of the globe. Part of civilization rests upon the ability to depend upon the integrity of the systems that society builds… and in this respect, the Internet and related technologies (especially the emerging area of nanotechnology and micromanufacturing) remain suspect.

At the Door of the Humblest Hut…

Citizens of the Agrarian and Industrial ages have more in common with each other than either with the emerging 'Netizenship of the Information Age. The physical properties that defined and limited public and private life prior to 1984 no longer constrain the new electronic age, and we are faced with evolving definitions of not only citizenship and economic participation, but of personhood.

The western understanding of privacy stems from the dictum of English Common law that (roughly paraphrased) "at the door of the humblest hut of the lowliest peasant, the King himself must stop and ask permission to enter." It was not the case that the King lacked the physical power to cross the barrier; nor is there overwhelming evidence that the King and his minions often bothered to stop or knock. Rather, the expression embodies a normative expectation that the King ***would*** do so.

Normative expectations are the product of social engineering, and the idea of privacy established that there was some physical space beyond the control of even Blackstone's observation "That the king can do no wrong is a necessary and fundamental principle of the English constitution." It evolved during a time when kingships aspired to absolutism in Europe, and it endured through contests between church and state, revolution and civil war, and the transformation of the economy from mercantilism to capitalism. The concept of privacy bestowed upon all persons, regardless of rank, station, or lot in life, some small degree of autonomy in the face of the overwhelming political forces of the day.

It was, of course, an extremely limited autonomy. The peasant who refused the King's request to enter paid a price, either immediately or as soon as he left the paltry safety of his humble hut. Nevertheless, that harsh truth is secondary to the importance of the symbolism: the humblest peasant possessed some quality, some right, to make even the juggernaut of royal prerogative pause in its course. And while it was doubtless honored more in the breach than the observance for much of its history, its normative power grew with time.

The delegates to the Constitutional Convention, with fresh memories of writs of assistance, Courts of Star Chamber, and the quartering of troops in private homes, wrote restrictions upon intrusive government actions into the foundation of this country's government. At the same time, Adam Smith's *The Wealth of Nations* articulated a larger transformation based in the notion of property (physical goods and chattels, including human slaves). Our jurisprudence contains numerous cases in which property itself stands against the power of the State, from the notorious Dred Scott case to the constellation of "United States versus Piles of Money" cases that paint a pointillist portrait of the drug war.

Until the 1960s, privacy vested primarily in the Fourth Amendment guarantee against unreasonable searches and seizures, which implicitly involve the physical world: persons, houses (places), papers, and effects. Social, medical, and technological advances coalesced in a variety of conflicts in that turbulent decade, and the notion of privacy also evolved (at least at law). The Supreme Court decision in Roe v. Wade provided a thumbnail sketch of those developments:

> The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as Union Pacific R. Co. v. Botsford, 141 U.S. 250, 251 (1891), the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist

under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment, Stanley v. Georgia, 394 U.S. 557, 564 (1969); in the Fourth and Fifth Amendments, Terry v. Ohio, 392 U.S. 1, 8 -9 (1968), Katz v. United States, 389 U.S. 347, 350 (1967), Boyd v. United States, 116 U.S. 616 (1886), see Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); in the penumbras of the Bill of Rights, Griswold v. Connecticut, 381 U.S., at 484-485; in the Ninth Amendment, id., at 486 (Goldberg, J., concurring); or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment, see Meyer v. Nebraska, 262 U.S. 390, 399 (1923). These decisions make it clear that only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty," Palko v. Connecticut, 302 U.S. 319, 325 (1937), are included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage, Loving v. Virginia, 388 U.S. 1, 12 (1967); procreation, Skinner v. Oklahoma, 316 U.S. 535, 541 -542 (1942); contraception, Eisenstadt v. Baird, 405 U.S., at 453 -454; id., at 460, 463-465 [410 U.S. 113, 153] (WHITE, J., concurring in result); family relationships, Prince v. Massachusetts, 321 U.S. 158, 166 (1944); and child rearing and education, Pierce v. Society of Sisters, 268 U.S. 510, 535 (1925), Meyer v. Nebraska, supra. (Section VIII)

"Privacy" expanded to include decisions, and while those decision had physical consequences (interracial marriage in Loving v. Virginia; the sale, purchase, and use of contraceptives in Griswold; abortion in Roe, etc.) it also began to extend to information. The case of Eisenstadt v. Baird is perhaps more salient than even Roe, dealing as it does with the dissemination of information that *implied* actions contrary to a state law. More recently, in Kyllo v. U.S., the Supreme Court robustly defended the Fourth Amendment concept of physical privacy even against "stand-off" technology:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, Silverman, 365 U.S., at 512, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search… At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. Silverman v. United States, 365 U.S. 505, 511 (1961). With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.

Writing for the Court, Justice Scalia noted:

> It would be foolish to contend that the degree of privacy secured to citizens when the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight

> has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. See Ciraolo, supra, at 215. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy… We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, Silverman, 365 U.S., at 512, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.

At the root of all arguments, Roe established the principle of "personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty' " were protected. While Kyllo anchored the concept of privacy in the 1780s (the cusp of the transformation from the agrarian age to the industrial), it also left the issue open by adding the proviso "at least where…the technology in question is not in general public use."

It is possible to envision a scenario in which Kyllo is swept aside. Adapting the technology to an on-street fire detection system, passively monitoring building heat via sensors on utility poles, would be a potential way to detect sudden changes in heat levels that suggest the early start of a fire. Such a system could augment or replace existing smoke- and fire-alarm systems, or provide a public alarm source in areas where privately maintained systems are unlikely. A street-mounted system would have an advantage at night, when occupants are asleep, and during periods when the occupants are away. In multi-family dwellings, fires that erupt in unattended common areas would be detected. And so, too, would any unshielded hydrophonic marijuana farms and other drug-production facilities using high heat.

Technology has fundamentally altered our perceptions of physical space. The Kyllo opinion also recapitulates an observation from the Dow Chemical case, noting that routine aerial flights created a different perspective of lands, a "third dimension" of surveillance that was once restricted to a two-dimensional plane (the Court in Dow made a distinction between commercial properties and 4th Amendment-protected private residences). To those routine airline overflights we must now add satellite photography and mapping, mini-cameras and radio-controlled model planes, both of which neutralize the ground-level fence as a defense of privacy. Widespread ownership of digital camcorders, cell phone cameras, telescopes, and the like all erode the expectation that our actions will not be recorded, and our ability to limit such intrusions. A similar argument is being made for the data-mining industry, which enjoys seemingly unrestricted access to information compiled from multiple entities to which we surrendered it for (we thought) a single purpose. Advocates of such unrestricted technology have asserted "You already have no privacy; get used to it," and they expect the rest of us to see the issue in their terms, agree, and acquiesce to the continual sifting of the intimate details of our lives.

It is at this point that the analogies to previous eras are most salient. We have never enjoyed total protection from the technologies of the age. There has always been a means to invade private domains, steal property, and cause various sorts of damage. "Privacy" is not a by-product of technology, and it need not recede because technological means are rapidly advancing. Privacy is a product of the social compact, and it is as essential to the social condition as is the integrity

of the individual corporeal body. We preserve it by deciding that it should indeed be regarded as a fundamental right, and using the alternate technology at our disposal—the law, and its instruments of enforcement—to insure that the social compact is honored by all.

Freeman Dyson recently observed that the age of Darwinian evolution has closed, yielding to the dominance of the human species and the shift to social evolution. The emergence of the cyber-*döppelgánger*, of an electronic identity (or identities) that is distinct from and independent of our physical self, is an important facet of that social evolution, one that is only now beginning to be charted.

On two fronts, our electronic selves are frightening. At one level, they are but cartoon representations of our real selves, abstract records that represent a part, but not the whole, of who we are. At another, they are not "us" but rather someone else's edited version of who we are. Our electronic selves are caricatures that serve not our purposes but those of other entities (often unknown and unrevealed to us). As such, they bind us with metaphysical chains that restrict our horizons and our futures.

An Imperfect Storm: The Privacy Wars

The Privacy Wars began in 2009 with the cloning of cell phones of a covert team of Department of Homeland Security operatives staking out California billionaire Serge Sourpuss, who had been falsely identified as a financier of the nascent pan-Islamic militancy. In a counterespionage coup worthy of the movies, the Personal Information Limits Front: Electronic Resistance (PILFER) sent false text-message commands complete with authentication codes to stakeout team members, luring them into embarrassing encounters with goop and slime and cartoonish devices usually not seen outside daytime television shows. The incident was captured digitally by the DHS unit's own cameras, which had also been cyjacked (cyber-jacked).

The Keystone Kops scenes of stealthiness meeting silliness were simultaneously web-cast, pod-cast to the next-generation EyePods, and jacked into several of the nation's cable networks. It preempted critical moments of the season's final episode of American Idol, whose broadcast was hijacked by PILFER for a second time.[1]

A more serious blow was the subsequent posting of the DHS unit's phone records and Blackberry files, worm-pulled from the secure service provider and similarly billboarded all over cyberspace. The phone records showed that the two "anonymous" phone calls that ostensibly provided the initial cause to open the inquiry (calls made to an Administration-friendly news entertainment blog called The Dregs Report) actually came from the unit itself.[2] Of far greater import, however, was the Blackberry information, detailing just how much of the billionaire's supposedly secure information had been obtained covertly—and illegally—by the squad. The Webline "Bug Brother Is Watching You!" appeared as wallpaper on the traveling web site.

Outrage over the emergence of a new "dirty tricks squad" poured fuel on a fire already smoldering from past abuses. The DHS unit chief's media-bestowed *nom du guerre* of "Donald Cy-gretti" invoked the ghosts of enemies lists and arrogance. Administration spokespersons' attempts to justify the squad's actions as a necessary counter-terror measure fell flat. Even friendly media representatives, using their real names, pointed out the absurdity of creating false enemies when so many real ones demanded the attention of the intelligence community.

By itself, the incident might have had the minor impact of brief embarrassment, like a lost

military laptop or a stolen SWAT team weapons van. However, it occurred three weeks after a similar widely publicized cyjacking of well-heeled donors to the Committee to Repeal the 25th Amendment at a fundraiser in Washington, D.C. While the cloning of cell phones had been identified as a security problem several years earlier with the theft of phone numbers from celebrities' cell phones, PILFER managed to crack state-of-the-art anti-theft devices that were installed in the cell phones of several government officials and "advisors" among the crowd (similar technology protected the cell phones of the DHS squad). The original Web-cast of the cyjacked information did not include the information stolen from the state-of-the-art phones: PILFER had not wanted to tip its hand to the DHS sting in California, which was still in its worm-pulling phase at the time.

The Wall Street Journal had trumpeted the protection of information of those individuals with the new cell phone technology (among whom were several "Pentium Plutocrats," chief executives of Internet and data-warehousing/data-mining companies) until Web- and Pod-casting services distributed a "Separated At Birth?" comparison the day after the California debacle. *The Journal* headline, the *Los Angeles Times* headline announcing the botched California raid, and the "protected" data were all available around the globe along with streaming video of the raid: PILFER withheld the protection-cell phone data from its original Washington release in order to maximize the Administration's embarrassment, anticipating that *The Journal's* response would come from someone.

Behind the scenes, as research in various archives has confirmed, the mining mavens were furious. Out of the public eye, their own oxen gored, the Pentium Plutocrats began a relentless campaign to increase federal penalties for data theft. Most of the model legislation protected commercial databases against intruders, but without including comparable protections for individual "identity data." In keeping with earlier legislative initiatives, most of the bills contained provisions for insulating commercial data collectors, storers, and processors from lawsuits by individuals who suffered damages from data and identity theft.

The Rise of The New Populists

The administrative *faux pas* still might have died the natural death of all scandals had it not been so closely linked to the accelerating problem of identity theft. The ripple effect of the ChoicePoint, Bank of America, Wells Fargo, and military database scandals continued unabated on local, regional, national, and international scales. Under pressure from the Pentium Plutocrats, Congress had resisted calls to create a central database for tracking identity theft cases. No one could account for how many electronic identities had been compromised, how many times the known victims' data had been sold and resold around the world, or how much monetary damage had been inflicted. All attempts to quantify the problem were blocked by the data warehouses' claims that first, it was proprietary information, and second, such inquiry would seriously compromise their equally proprietary efforts to improve their protection of their customers' identities.

Then the media found their poster child: an educated, articulate, telegenic, middle-class widow of an Iraq War medal-winner who was evicted from her home because of financial difficulties stemming from unresolved identity theft. She had kept meticulous electronic records with hard-copy backup, supplemented by legally recorded tapes of her latter-day telephone conversations with industry representatives to whom she turned for resolution

of the problem. Despite her efforts, the legal limbo of her finances persisted until the home was repossessed.

When she turned to the media for help, she instantly became Anywoman. That nickname stemmed from her passionate declamation to Paula Zahn: "I have never been unemployed. I have never spent more than I earned. I have always taken the industry's recommended precautions, and aggressively sought to upgrade my protection. I have been blessed with enormously supportive family and friends throughout these ordeals. And I am on the brink of losing everything because my identity was stolen and no one seems to be able to fix it. If this can happen to me, it can happen to any woman!"

As the news media filmed sheriff's deputies moving her furniture to the sidewalk, Anywoman turned to the cameras with a blistering denunciation of the "ownership society," excoriating the Congress for being in the pocket of the Pentium Plutocrats, and asking the rhetorical question "What are my alternatives so that this never happens again?"

That question ignited the blogosphere. More and more victims of identity theft came forward, highlighting more and more instances of industry inability (and in some cases, unwillingness) to correct the problems. The mainstream media lost control of the story, and were reduced to reporting on the contents of the blogosphere as the issue came to dominate the national conversation.

Populist candidates threw their hats into the ring of the upcoming elections, demanding a potpourri of additional computer security, restrictions on data-sharing, and avenues of recourse for victims of identity theft. Both traditional polls and the blogosphere showed them attracting a substantial minority of support for their essentially single-issue campaigns, and incumbent politicians began to propose bills to steal the issue from the populists.

The Industry Response

The data mining industry responded with assurances of higher-technology solutions, incorporating biometrics. They stayed on-message with reminders that none of the information "lost" was actually private (having been voluntarily surrendered in the first place and shared in strict accordance with the small print of agreement forms that the affected consumers had presumably read and understood), that identity theft had occurred even under paper-driven systems, and that the industry was working very, very hard to assure their customers. A smaller number attempted to make the case that "transparency" actually protected individuals because the more information that was available, the more it could be verified in the light-speed networks.

The Administration joined in the defense of the industry by linking the identity theft issue to homeland security's long-stalled proposal for a national identity card predicated upon biometrics. A prototype was to be distributed on a voluntary basis, combining personal, financial, medical, and biometric scales similar to the DNA-based new-generation dog tags of the U.S. military. The U.S. Attorney General received the first prototype I.D. card in a prime-time Rose Garden ceremony, and made the historic first withdrawal of money (a modest fifty dollars) from a wireless ATM brought to the Rose Garden for the occasion.

Two days later, PILFER broad-, web- and pod-cast the Attorney General's personal data, including her biometric security code. Accompanying it were the account numbers and passwords of the bank accounts PILFER had established with it in all fifty states and the Virgin Islands, under the name "Eli On" (for "E-Lie On..." according to PILFER'S announcement). Each account held a modest fifty dollars, electronically

transferred from the A.G.'s original account. The new account information was revealed "so that the Attorney General is not permanently deprived of her rightful property," according to PILFER's accompanying manifesto. [3]

The tabloid headline "Bluetooth Blew Truth" became the rallying cry of the then-amorphous resistance to a national ID card. Sensing blood in the water, the news entertainment media began running stories headlined "The Demise Of The World-Wide Web" and "What Is The Net Worth of The 'Net?" The blogosphere became a cauldron of conspiracy theories, most of them intricately constructed more of fear than of fact.

An obscure academic in Ohio was asked by a reporter about the industry's assertion that electronic transactions were really no different than their face-to-face predecessors. His answer was picked up by the news wires, then by the blogosphere: "Some one has always known. What is different is that now, anyone and everyone can know." An anonymous blogger added "Transparency Is Privacy" to George Orwell's famous triad from 1984 ("War is Peace / Freedom is Slavery / Ignorance is Strength"), and the mantra spread like wildfire on bumper stickers, backpacks, and e-mail tag-lines.

A growing number of Americans decided that they did not wish to live in a glass house or a "transparent" society. While poll support for the populist candidates grew steadily, a grassroots economic self-help stratum quickly sprang up, spearheaded by credit unions and labor unions, and quickly joined by small banks. On-line tax filings to the IRS fell precipitously, replaced by paper reporting. A Senator who was a staunch advocate of the banking and data-mining industries introduced a bill attempting to amend the tax code by requiring electronic filing. This ignited a blistering torrent of e-mail and snail-mail, and the bill died in committee.

The European Union Electronic Underground (EU2) began mimicking the cyber-attacks of PILFER, with almost daily exposés and manifestos published under the *nomme du guerre* of its putative leader, Pro Bono. Though their exposés were heavily censored so as to minimize the jeopardized data (flirting with but not stepping over the European Union's own privacy laws), they had the desired effect: the American cyber-dilemma became the most visible topic in Europe as well, eclipsing the travails of England's royal families and drowning out the ramblings of the neo-Nazi movement. American corporations came under heavier criticism from the European Union for their shoddy protection of consumer data, with threats of boycott and a suit before the World Court to protect European citizens' transactions in accordance with European standards.

The Redefinition of Homeland Security

To no one's surprise, the data-mining industry's response to the turmoil was to link their lucrative business to homeland security. Flogging the concept of "transparency" as a defense against both identity theft and terrorism, they continued to maintain that no changes could be made to their business without catastrophe occurring. However, in a particularly acrimonious face-to-face exchange with an industry flack during a rally on the Mall, Anywoman changed the debate with a single question: "How can the homeland be secure when the home is not?"

That question effectively ended the first round of the privacy wars, and redefined the terms of the debate. A new discourse began, instigated in cyberspace and quickly distributed by neighborhood-based papers that served areas with little or no Internet access. A code of civility evolved around an initially small debate among three primary bloggers: General Net Ludd (presumed by many

to be either the de facto leader or the collective avatar of PILFER), a conservative industry defender whose cybername was ALLCAPP (like his posts, which carried the tagline: "WHAT'S BAD FOR GENERAL BULLMOOSE IS BAD FOR THE U.S.A."), and Phydeaux ("In cyberspace, nobody knows you're a dog," the caption of an old New Yorker cartoon) who represented the vast majority of users concerned about the short- and long-term implications of data-sharing and identity theft, but bewildered by the rancor of the debate.

One of the CEOs of the computer industry sponsored an open forum, PlebiSite, initially inviting the three primary spokespersons to refine the edges of the debates with a blog entry each week. Their three-way dialogue quickly accelerated to an entry each day, which drew the attention of hackers. The nominally secure site, open to the three invited participants but read-only for the general public, was quickly stripped of its security devices by Kan Key-See and The Merry Phreaksters.

Intended to be a three-way debate, PlebiSite immediately became an open forum that served as a clearinghouse of public concern. Anywoman joined the three main spokespersons on occasion, but most of the input came from short, pithy statements or questions from citizens on all sides of the issue.

The anonymous blogger who adopted Legion as his or her cyber-name ("For we are many") took the first step toward reorienting the public's consideration of the privacy issue by invoking the Preamble to the Constitution: "provide for the common defense and ensure domestic tranquility." Reminding the nation that the two attacks on the World Trade Center had been mounted because of its symbolic role as the center of the American economy, Legion offered a series of rhetorical questions about the impact of the globalizing economy on the average American. Net Ludd and Anywoman seized on those questions to leverage their own attacks on the government and the financial community's use of consumer data, respectively, and Legion's input was swiftly shunted aside into a sidebar thread.

The mainstream media deemed the resulting exchange of views "the new national conversation," and began to track its themes. Concern over the manipulation of personal data replaced tirades about "privacy" (ironically mimicking earlier rhetoric from aborted attempts to redefine Social Security as "private" and "ownership"). Six segmented dialogues ensued, focusing on the resale of information surrendered for credit; medical information; public surveillance by private entities and corporations; covert surveillance by the government acting on probable cause; similar surveillance by government entities in a "proactive" role, which incorporated the idea of a national ID card; and the industries of data-mining and academic research.

The surveillance debate flared intensely at first, fueled by one of the ACLU's perennial challenges to a local police department's practice of videotaping political demonstrations. ALLCAPP challenged the ACLU to cite any cases since 1984 when such videotaping had led to any prosecutions, or even curtailments of individuals' right to freely assemble, speak, or petition their government for redress. Phydeaux deflected the issue somewhat by pointing out that the same practice had also helped bring to justice several serial arsonists, the provocateurs who had attempted to turn peaceful protests violent on at least one occasion, and scores of individuals who had committed serious acts of assault and vandalism during violent protests against the WTO and other international bodies.

Then one of the outspoken proponents of surveillance proposed that CCTV be installed in public toilets "to protect the unborn" by documenting the abandoning of newborns. The resulting flame war led to monitoring of the

PlebiSite postings, and to self-moderation by the remaining posters. After a renowned Harvard-based attorney posted a synopsis of the Supreme Court cases dealing with privacy, most accepted the lack of privacy in public space and the workplace, as well as the government's overriding interest in conducting surveillance for criminal cases. A trailing debate over the permanence of records and the limits on dissemination of images merged with the larger umbrella of medical and credit privacy.

Credit Information. Given the pervasive need to use credit in modern society, this debate soon turned on whether credit information should be established on an Opt-In or Opt-Out basis. ALLCAPP stayed on-message for the industry mavens, touting the "opportunities" that would result for consumer and industry alike if credit information could be shared. He stridently advocated for the current status quo of Opt-Out, invoking images of Jeffersonian yeomen farmers being informed and advised of the things that concerned them and their government.

Net Ludd countered with a salvo of federal laws and their corresponding regulations, in brief, asking rhetorically how anyone who actually worked for a living could individually manage to stay abreast of developments that highly-paid specialists tracked for industry. He argued for simplicity from the consumer's side: Opt-In allowed those who wanted to be contacted to participate, but the default stance should be that the consumer had an equal stake in the purchase of credit with the provider of credit. Their proprietary relationship should be limited as a matter of law to that purchase, and extend no further.

After a flutter of postings asking if Ludd "worked for a living" himself, ALLCAPP responded with lengthy summaries of credit defaults, bankruptcies, and delinquencies. Those abuses of credit, he argued, made data-sharing mandatory. Phydeaux countered with a mild question of whether anyone knew how many of the bankruptcies resulted from identity theft.

In response, PlebiSite was flooded with posts from individuals who had suffered financial losses from both identity theft and uncorrected errors in their credit reports. A second wave of new participants followed a week later, after the mainstream media picked up the story. Additional horror stories about criminal histories established under stolen identities began to sprinkle the discussion.

Medical Information. A parallel thread, at first unconnected to the identity theft discussion, had been muted until the flood of identity theft stories. The medical discussion then shifted from hypothetical Gattaca-like denials of insurance coverage and employment opportunities. Many contributors reported receiving advertising for medications directly related to conditions they had thought were known only to their physicians.

Four separate mainstream media outlets jumped on the new thread, pushing several long-term investigative reporting efforts into the spotlight. The interconnected associations of the medical, pharmaceutical, and insurance industries centered on several of the high-profile data-mining corporations already being pilloried in the credit and identity theft threads.

The untimely death of one of the representatives from a western state intervened. Six vocal privacy advocates filed as independent candidates in a special election held to fill his office, but early poll returns indicated that business-backed candidates from the major parties were profiting from the split vote for the opposition. The second-leading privacy candidate withdrew in favor of the issue's front-runner, giving a bravura performance that clearly wrote the privacy agenda's manifesto for the state's constituents. Several other privacy advocates followed suit, giving the privacy slate a

strong plurality.

The overall economy of the state was healthy, individual bankruptcies and a series of farm foreclosures in the northern part of the state elevated data privacy to the signature issue of the election. Though party representatives attempted to define the election as a two-way race based on family values, the media and the blogosphere kept the privacy issue, and the independent candidacy, at the forefront. Behind a series of ad hominem attacks against the Independent, the major party machines quietly conceded the ground, and responded. They launched a heavily funded campaign against any restrictions on current business practices, dominating the mainstream airways but thoroughly derided and lampooned in cyberspace.

In the only three-way debate among the major candidates, on the eve of the election, both party candidates gave strong defenses of existing privacy practices, only to see their supposedly private data highlighted on the screen behind them: PILFER had engineered another cyjacking.[4]

The following Tuesday, the independent candidate won more the 53 percent of the votes cast, in an election notable for its high turnout. The mainstream media trumpeted the victory as a mandate for privacy, noting that there were no other high-profile stakes in the election. Upon arriving in Washington, D.C., the newest representative immediately filed a PILFER-designed bill that gave control over individual data to the individual, and required specific permissions for any data sharing. All secondary recipients of data, whether credit bureaus or insurance companies, would be bound by the specific requirements of the primary surrender of data.

Within 72 hours, the bill was festooned with amendments that eviscerated the spirit of the bill, promoted on the basis of "transparency," though there was little evidence of anything behind them but exempting the data industry from the main provisions of the bill. The House leadership rushed the bill to committee for a vote.

The network of privacy advocates that had evolved from the PlebiSite discussions anticipated such a reaction. Congress-watchers wirelessly blogged each of the amendments almost as soon as it was offered. Snippets of each sponsor's proposal and speech filled the blogosphere, and a flood of e-mail and snail mail filled congressional mailbags and inboxes, railing against the changes. The Independent withdrew the bill with a flourish in a media-heavy press conference, excoriating the added provisions and gently chiding their sponsors.

A network of political operatives with ties to billionaire Sourpuss (but not to PILFER) quickly filed recall petitions against amendment sponsors in every jurisdiction where recall was available. The recall petitions were supplemented by a rash of independent filings for the upcoming congressional races across the country. Under this unanticipated pressure from privacy advocates, few in the national legislature were willing to support openly any bills supporting unrestricted data sharing.

The various state-based privacy coalitions united under an umbrella group formed in Maine, PRIVAC-E, allowing Sourpuss and PILFER to remain apparently peripheral to the larger movement. Though he channeled some funds to PRIVAC-E through above-board means, Sourpuss saw the advantage of a grassroots organization that had plausible deniability in case PILFER's underground campaign was exposed. PILFER returned to Fifth Column status, staying out of the public eye until the anticipated counterattack by the data industries and their allies.

The Counterattack

The final stages of the battle were fought in the run-up to the mid-term election. When the discussions of identity theft problems faltered on PlebiSite, the data mining industry launched a media blitz promoting "transparency" as a means of preventing and surviving identity theft and other misuses of personal data. A spate of industry-sponsored posters filled PlebiSite with messages that hawked the inevitability of identity theft problems under the ineffectual patchwork of laws and regulations that plugged holes well after the fact. Talk shows were suddenly filled with "experts" who pronounced the old notions of privacy dead, the inevitable casualties of the globalization of the economy. The message was consistent: only full exposure, in multiple locations that could be checked and verified at lightning speed, could thwart attempts to purloin or alter personal data. The industry promoted the potential benefits to the economy that would be derived from reducing fraud, hinting at lower consumer prices across the board, from retail to auto insurance to medical insurance.

At the same time, Administration supporters of the industry brought forth a series of initiatives under the banner of homeland security. A series of cases of attempted terrorist assaults that allegedly were intercepted or otherwise neutralized were promoted in news conferences. Spanning almost a full decade, from the months immediately following the 9/11 attacks to December of the preceding year, the incidents were linked by assertions that data mining had led to the identification of the terrorists. The consistent message was that the ability to sift through credit card transactions, cell phone traffic, library and Internet use, and in one case GPS tracking of a rental vehicle had kept America safe. An underlying theme hinted that the same techniques were protecting Americans from criminal activity.

PILFER had anticipated the general outlines of the industry's campaign, but held back its response for several weeks. During that time a blizzard of objections filled the blogosphere and dominated traffic at PlebiSite, a vociferous if uncoordinated vox populi rebuff of the industry's and the administration's assertions. The tail wagged the dog at first: most of the early posts ignored the covert tracking of terrorists (of which the general public knew nothing) and focused on the identity theft issue that they knew only too well. A radical economist who had been employed in several Ivy League schools commandeered an outdated advertising slogan—"I am the C.E.O. of Me!"— to put forth a strident philosophical view that by advantaging corporate use of personal data, the administrations of several presidents had undermined the economy by suppressing both control and decision-making, and thus creativity, at the most important level of the economy. No one paid any attention to the convoluted economic proofs offered by the economist, or to the more well-grounded rebuttals from mainstream economists, but the slogan quickly became the rallying cry of the opposition.

By trying to hijack and redirect the national discussion, the industry inadvertently highlighted the pervasive encroachments upon personal privacy, and reignited the moral indignation of the citizens watching the unfolding drama. A couple of the new PlebiSite contributors who were on the industry payroll were outed by a freelance whistle-blower who had once worked in the industry. She posted memos outlining industry plans (created several years earlier) for a "transparency" campaign in case Congress ever brought pressure as it had against the tobacco industry: some of the wording of that campaign's "Concerned Citizen Letters" were identical to posts on PlebiSite.

Industry spokespersons began an immediate

campaign to discredit the whistle-blower as a disgruntled employee, hinting that she herself had posted the CCLs she criticized. They also attempted to turn her message back on itself, asserting that transparency rules, the industry's participation in the debate through their agents would have been widely known and thus no scandal whatsoever.

PILFER held back until the character assassination reached a peak, then unleashed a barrage of intra-industry communications provided by moles within the industry (some were in fact disgruntled employees; others were PILFER operatives who had worked in the industry for years, including one of PILFER's founders). At the same time, PILFER posted pending legislation that purported to provide transparency protection, detailing the ramifications of each and every provision that alleged consumer protection, but actually constituted insulation of the industry against lawsuit by consumers.

Putting the data industry under a microscope was bolstered by a general exposé of existing laws and proposed legislation that impeded inquiry into corporate finances and deal making. The slow swell of stealth legislation, riders, and amendments that had undone most of the Sarbanes-Oxley law had been the original issue around which PILFER had organized, and it had extensive files with clear-cut points of attack.

Integrating fragmented investigation by a score of smaller citizen advocacy groups, PILFER jumped on the "CEO of ME" bandwagon. In its most mainstream publicity campaign to that point, PILFER hammered home the discrepancies between the protections afforded the Pentium Plutocrats and their corporate brethren, and the exposure in the name of "transparency" that was inflicted upon the citizens of the nation. The campaign morphed the CEO image into a new slogan, "With Transparency and Justice For All," demanding that the corporations be subjected to the same levels of transparency as the citizen "Me-E-Os." After two weeks of bulleting the disparities, PILFER put forth model legislation for achieving just that. Sitting members of Congress were swift and almost unanimous in their denunciation of the model legislation, which essentially meant that PILFER had promulgated the platform of the opposition in the coming election.

The provisions of the nascent Patriot Act V were also dissected, outlining the two-pronged assertion of increased federal snooping power and restrictions upon Freedom Of Information provisions. Anywoman's "how can the homeland be secure when the home is not?" question dominated the debate, however: most citizens could find common ground with those whose lives had been thrown into turmoil by data theft and misuse, where they had little emotional connection with government intrusion. Nevertheless, it remained an important, and strident, sub-thread that periodically augmented the more personal discussions on credit and medical histories. As one historian has noted, looking backward on the period, the FOIA thread continually reminded citizens of the role government had played in allowing the credit situation to evolve, and of the obstructions it had placed on ordinary citizens' ability to regain control over their lives. While few bought into the more revolutionary claims that the national government was a wholly-owned subsidiary of business, many recognized and remarked upon the need to control government in order to control business excesses.

A week before the elections were to be held, Legion rejoined the debate, posing the question, "What becomes of 'private property' if there is no privacy?" She or he drew out the invisible threads of the industry proposals, noting that all of them contained a tacit assumption that information about a customer or client constituted the agency's

"proprietary" property —a word, Legion noted, whose dictionary definition meant "ownership." Legion then posed the second, more important question: "When did I become a slave? That so-called 'proprietary' information is an electronic version of me, and it is available to be bought and sold… not down the river, but down the data stream. How is it that they have such control over me, and I do not? In this matter, I think, Anywoman and I have common cause: allowing our electronic selves to be converted to others' property nullifies our autonomy, effectively cancels our citizenship, and renders us slaves, not to a plantation master, but to corporate interests. And yet we are supposed to have a constitution that prohibits slavery. The time has come, to reassert our rights as free men and women. We know that the technology exists that makes this possible. The technology also exists to make armed robbery possible. We prohibit that misuse of hard steel technology, and it lies within our power to prohibit the misuse of electronic technology."

Merged with the "CEO of Me" campaign, Legion's questions dominated the remaining blog traffic on the election's eve. The populist candidates seized on the issue, and pushed out rapid position papers reaffirming the individual's right to be protected from electronic slavery. PRIVAC-E sponsored agile sound-bytes highlighting the difficulties individuals had experienced in regaining control over their finances, highlighting the exceptional deference that business gave to their electronic profiles and faux histories, with little or no regard for the real-world (paper) evidence that was provided by real-world people. The industry replies (detailing instances of fraudulent claims, among other things) were strongly worded and well-documented, but fewer in number than the horror stories that PRIVAC-E summarized and re-posted.

And then, on a clear, bright day in early November, America awoke, and went to the polls.

Endnotes:

[1] *American Idol* was targeted after ostentatious announcements by the various network and cable executives that the infamous spoof episode "*America, I'm Dull*" could never happen again. In fact, a 'deja view' was already in the works for an episode of *The Simpsons*, titled "*America, I'm - D'OH!*" Although PILFER was publicly blamed for the original broadcast override, the group never took credit for it, and the cast of digitally-disguised characters on the show spoke and "sang" with accents that suggested a Slavic origin.

[2] The fact was that the phones had already been cyjacked by PILFER, who made the instigating calls without the DHS unit's knowledge. The cyjacking took place in response to the original intrusion into Sourpuss's records. Although the "information" about the pan-Islamic financing in the files was false—the investigation team actually hacked a honey pot that Sourpuss and PILFER established before the billionaire began his public campaign against the Administration's Middle East policies—the fact of the intrusion took on dimensions greater than its individual merits. Sourpuss was never prosecuted for the alleged bankrolling of "terrorists," and the federal government failed to substantiate any of the nominal leads provided in the honey pot. The full story would not be revealed until Sourpuss's death in 2011, by which time the California incident had become the Blitzkrieg of a new cyber-war against perceived abuses both public and private, and PILFER felt secure enough to acknowledge that in fact Sourpuss was bankrolling PILFER, not the pan-Islamic movement.

[3] Intent to permanently deprive the rightful owner of property is an essential mens rea element of the crime of theft, so PILFER's street theater had a self-serving element as well.

[4] Though all three candidate's finances were bared, the Independent candidate was a private citizen of modest means, with very little to hide. He had offered to make the information public early in his campaign, as an "I have nothing to hide and I still want my privacy!" gambit. He was contacted by PILFER almost immediately, and as his candidacy grew, the monkey-wrenching plan was conceived.

References

Dyson. Freeman. (2005). *The Darwinian Interlude*. Retrieved from < http://www.technologyreview.com/articles/05/03/issue/magaphone.asp >3 March 2005.

Feuer, Alan, and Jason George (2005). "Internet Fame Is Cruel Mistress for a Dancer of the Numa Numa." *The New York Times*. Retrieved from < http://www.nytimes.com/2005/02/26/nyregion/26video.html >on 26 February 2005.

Reuters (2003). *No Surveillance Tech for Tampa,*Retrieved from < http://www.wired.com/newspolitics/0,1283,60140,00.html > on 21 August 2003