# *The Future of Privacy (Law)*
## *[or CSI:ID -- when your digital DNA (figurative & literal) goes viral]*

G. Erik Furlan
Elon University
M.A. Interactive Media
2009-2010

# *The Future of Privacy (Law)*
## *[or CSI:ID -- when your digital DNA (figurative & literal) goes viral]*

Abstract:

A futures-thinking approach toward the examination of the privacy issue will be taken in an effort to out in front of the issue, to be better prepared to address potential concerns. Instead of issues of privacy being addressed proactively, in large part they are addressed in a reactive fashion. With technology outpacing the current privacy "action plans" (aka legal and structural/systemic privacy protections), large grey areas are forming, leaving key concerns unaddressed.

Many take privacy for granted, viewing it as a right, along the lines of freedom of speech and the right to bear arms. Yet, an explicit mention of a right of privacy cannot be found anywhere in the complete text of the United States Constitution. However, over the years, legal cases and Supreme Court rulings have, for lack of a better word, created a right of privacy, one that is constitutionally protected.

Investigation into the history of privacy, its development into an implied constitutional right, will establish the foundation of the idea of privacy in the United States. An examination of current literature will help establish a base of what some of the current privacy concerns are and what overarching questions about privacy protection need to be answered. Privacy opinion leaders and privacy advocates will be consulted as well, taking the pulse of privacy, looking at what the potential privacy issues may have to be faced in the future.

There needs to be a shift in the approach to addressing issues of privacy. Technology is lapping the current action plans in place to handle privacy concerns. Solutions have to be more proactive instead of reactive -- instead of waiting for the problems to appear to figure out a solution, there needs plans in place for the possible, having on hand methods and systems to deal with issues that arise. Technological development isn't going to stop and privacy policies need to get out in front of the curve.

# *The Future of Privacy (Law), or CSI:ID -- when your digital DNA (figurative & literal) goes viral*

Ask one hundred people for their thoughts on privacy and you are likely to get one hundred different answers. Those of the younger persuasion have a different concept of privacy than prior generations, thanks in large part to the technological world in which they live; a world where the sharing of personal, sometimes intimate details of their lives isn't a big deal, but rather the norm, perhaps even expected in order to function socially.

Many take privacy for granted, viewing it as a right, along the lines of freedom of speech and the right to bear arms. Yet, an explicit mention of a right of privacy cannot be found anywhere in the complete text of the United States Constitution. However, over the years, legal cases and Supreme Court rulings have, for lack of a better word, created a right of privacy, one that is constitutionally protected.

These static and dated concepts of privacy are on a collision course with technological development, failing to adapt to the changing times. Issues of privacy are typically addressed in a reactive fashion (in response to a specific question) as opposed to a proactive fashion (anticipating potential questions and planning for them). The fact of the matter is technology is outpacing current privacy definitions and legal protections, leaving too many gray areas with no clear guidelines to address concerns, such as:

> With the permanent nature of the Internet – once its posted it's out there for good – is it possible to take something back? Is it feasible to demand others in possession of it to return or destroy it? Can you put the genie back in the bottle once something has gone "viral?"
>
> Is it possible to have over-arching privacy standard, given the generational differences in the expectations of privacy? Can privacy be violated if something was posted, like via Facebook, willingly? Is a new definition of 'privacy' and what is considered 'private' needed in this new, networked, connected world?

The journey to address these concerns begins with an examination of past issues and resolutions in the privacy debate – how the constitutionally protected right of privacy came into existence via Supreme Court decisions. With that history in place, examples of current privacy problems will be examined, highlighting the fact that the legal privacy protections established as part of the creation of the right of privacy are not compatible with the new privacy problems of the digital future. From there, expert opinions will launch the look toward the future, trying to determine possible solutions to ensure there is a future of privacy, that privacy continues to live on as an implicit constitutional right.

Ultimately, there needs to be a shift in the approach to addressing issues of privacy. Technology is lapping the current protections in place to handle privacy concerns and privacy policies need to get out in front of the curve before it is too late to even catch up.

Scott McNealy, CEO of Sun Microsystems in 1999, became known for saying "You already have zero privacy. Get over it." Was he right then? Is he now? Is this an inevitable scenario or can privacy still exist in the (digital) future? We shall see.

***Take a right on privacy and go straight till you get to the OBGYN – Privacy Past***

Before any thorough examination of the future of privacy can begin, one must examine where it has been. Specifically, looking at the evolution of the right to privacy in the United States legal system, since "the word *private* is enunciated in the U.S. Constitution as part of the phrase "private property," [but] the term *privacy* is not specifically found in the Bill of Rights or in the body of the Constitution itself" (Johnson, 2005, p. 54-55).

Early in United States history, specifically in pre-Civil War era, the understanding of privacy, at least from a legal perspective, "was as a personal one, related more to the circumstances of a person's immediate physical environment (essentially the home) than to an assertion of a generalized legal, moral, or natural right" (Johnson, 2005, p. 57). The beginnings of the idea of a right to privacy in the more generalized sense have been traced back to an essay that appeared in the *Harvard Law Review* in 1890. The authors of that essay, Louis D. Brandeis, the future Supreme Court justice, and Samuel D. Warren, his former law partner, asserted that "the common law secures to each individual the right of determining, ordinarily, to what extend his thoughts, sentiments, and emotions shall be communicated to others" (Rosen, 2000, p. 5). The two also explained that the same legal principle that barred prosecutors from examining letters, books, diaries and other private papers should also be applied to gossip columnists, preventing them from publicly ruminating about the sex lives of private citizens. "They called that principle the right to an "inviolate personality" and said that it was part of the more general "right to be let alone" (Rosen, 2000, p. 5) [the concept of the right to be let alone coming from an 1879 volume on tort law by Thomas Cooley (Johnson, 2005, p. 57)].

Arguably, the major impetus behind the writing of the essay was Brandeis and Warren's concern over "the press's intrusion into one's private life that could lead to loss of reputation or the divulgence of embarrassing personal facts. … [and] the unauthorized publication of pictures of individuals (Johnson, 2005, p. 60). Take a moment and examine the last sentence, especially the concepts of "loss of reputation" and "the divulgence of embarrassing personal facts." Those are nearly identical to the concern being raised today in the era of YouTube and Facebook. The idea of how you are viewed online and the risks of personal facts becoming public knowledge were just as crucial then as they are now in the time of online overshare. This new direction of privacy will be revisited later in this paper.

A case can be made that the first legal decision involving a right to privacy was the 1905 case of *Pavesich v. New England Life Insurance Co*. (Johnson, 2005, p. 61). Paolo Pavesich successfully sued over the unauthorized use of his photo in an advertisement for New England Mutual Life Insurance Company. It was here that the right to privacy began to move beyond the property-based definition into the realm of a personal right under the auspices of personal liberty.

In the years preceding and following *Pavesich*, several cases skirted around the issue of privacy without necessarily specifically defining it or applying it as a personal right (some feel that the groundwork for the "penumbra analysis" that would appear in *Griswold v. Connecticut* was laid here):

- *Boyd v. U.S. (1886)*
- *Weeks v. U.S. (1914)*

- *Silverthorne Lumber Company v. U.S. (1920)*
- *Meyer v. Nebraska (1923)*
- *Pierce v. Society of Sisters (1925)*
- *Buck v. Bell (1927)*
- *Olmstead v. U.S. (1928)* (Johnson, 2005, p. 63-66)

The case that would take privacy across the "constitutional threshold" (Johnson, 2005, p. 76) wouldn't come until 1961 with *Mapp v. Ohio*. The case involved the warrantless search of Dollree Mapp's house, looking for a suspected bombing fugitive. While carrying out the search for the fugitive, Cleveland Police found a suitcase with pornographic drawings. Mapp claimed the suitcase was not hers and she was unaware of its contents. Mapp was arrested and convicted for possessing obscene material. The Supreme Court eventually overturned Mapp's conviction, essentially applying via the Fourteenth Amendment the Fourth Amendment protection against unreasonable search and seizure to state as well as federal courts. Some viewed this as a legitimization of the right to privacy that had been inferred from interpretations of the Fourth Amendment since it was being expanded by means of the due process clause of the Fourteenth Amendment (Johnson, 2005, p. 76). In the majority opinion of *Mapp v. Ohio,* Justice Tom Clark "made explicit, albeit confusing, mention of a right of privacy: "The right to privacy, when conceded operatively enforceable against the States, was not susceptible of destruction by avulsion of the sanction upon which its protection and enjoyment has always been deemed dependent under the *Boyd, Weeks* and *Silverthorne* cases," stating later 'privacy [is] no less important than any other right carefully and particularly reserved to the people'" (Johnson, 2005, p. 75-76).

So, there it was, constitutional evidence of a right of privacy, right? Not exactly -- privacy cases had primarily dealt with law enforcement procedure and case-by-case problems. There still wasn't a definitive case that would make the personal right of privacy explicit. Enter *Griswold v. Connecticut*.

In *Griswold*, a Connecticut law prohibiting the use of any pharmaceutical or device to prevent contraception was under the microscope. Estelle Griswold, Executive Director of the Planned Parenthood League of Connecticut, and Dr. C. Lee Buxton were found guilty of violating the statute when they opened a birth control clinic in New Haven, CT. In the appeal to the United States Supreme Court, it was argued that the Connecticut statute violated the Fourteenth Amendment's 'due process' protection. The conviction was overturned and the constitutional right of privacy was born. Justice William O. Douglas outlined his rationale for the right in his *Griswold* opinion:

> The First Amendment has a penumbra where privacy is protected from governmental intrusion … Specific guarantees in the Bill of Rights have penumbras, formed by emanations from the guarantees that help give them life and substance …. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one … The Third Amendment in is prohibition against the quartering of soldiers "in any house" in any time of peace without consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches

> and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution of certain rights, shall not be construed to deny or disparage others retained by the people. (Bartee, 2006, p. 203)

So, the right to what was dubbed "marital privacy" had been explicitly defined. That begged the question, what about contraceptive access to the unmarried or minors? In *Eisenstadt v. Baird, "…* the High court upheld the appellate court ruling and vindicated Baird's right to distribute contraceptives to unmarried persons. … Justice William Brennan, writing the majority opinion in *Baird*, ruled that the Massachusetts law prohibiting the dissemination of contraceptives to unmarried persons violated the equal protection clause of the Fourteenth Amendment" (Johnson, 2005, p. 198-199). *Cary v. Population Services Int'l* (1977) extended the same argument in regards to minors (Bartee, 2006, p. 207).

This train of reproductive privacy thought continued, encompassing the abortion issue crystallized by *Roe v. Wade*. "The privacy right to sexual activity for pleasure, not procreation, became settled law. The succession of reproductive privacy cases moved to encompass abortion rights as well as those of birth control. *Roe v. Wade* (1973) as reaffirmed in *Planned Parenthood of Southeastern Pennsylvania v. Casey* (1992) established this right …" (Bartee, 2006, p. 207). "What needs to be stressed is how *Roe* stretched the constitutional right of privacy enunciated in *Griswold* and modified in *Baird*. In [Justice Harry Blackmun's] majority opinion … the Court ruled that the Constitution protected a woman's right to an abortion in the first three months of her pregnancy but allowed the state to regulate abortion during the remaining two-thirds of her term" (Johnson, 2005, p. 202). This decision was grounded in the right of privacy. "Blackmun made reference to a long chain of Court decisions and individual justices' opinions involving privacy going back to 1891. "[T]he Court has recognized," Blackmun wrote, "that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution"" (Johnson, 2005, p. 202).

Before we travel any further into the morass of privacy, let's step back and review. Essentially, the right of privacy that was explicitly spelled out in *Griswold* (and refined in subsequent cases) was born out of reading between the lines of the amendments in the United States Constitution:

- First -- "one's ideas are one's own and may not be dictated by governmental power or censured if expressed. Logically, this reading of the First Amendment may entail that one possesses the liberty not to share one's thoughts with others, especially with the government." Also "right to assemble … petition the government … rights not to associate with certain people and not to have the identity of one's affiliations or associates made public."
- Third – "prohibition of quartering of soldiers in private homes during times of peace stems directly from the fear of such violations of private space that concerned the writers …"

- Fourth – "unreasonable searches and seizures" – "safeguards the private papers and personal possessions of individuals, unless proper warrants are issued or probable cause is demonstrated …"
- Fifth – "it affords individuals the right not to be compelled to give evidence that might be used against them in criminal proceedings. Privacy is thus *implied* by language in selected portions of these several amendments."
- Ninth (the "people's rights clause") and the Fourteenth (the "due process clause")

Scott Gaylord, Associate Professor at the Elon University School of Law, concurs with this perspective on the formation of a right to privacy:

> "Although expressly recognizing a right to privacy, the United States Supreme Court (the "Court") initially had trouble deciding in what portion of the Constitution it was located. Because it is not an "express" right, the Court held that it emanated from the penumbras of various other rights. That is, the right to privacy was implied from other express rights found in the various Amendments [First, Third, Fourth, Fifth, Ninth and Fourteenth]. Since the early cases (e.g., *Griswold* and *Roe*), the Court has viewed the right to privacy as an established right without worrying so much about locating that right within a specific provision of the Constitution." (personal communication, December 3, 2009)

By now one has to be wondering, 'what on earth does a teen being able to get the pill have to do with the future of privacy?' In a word – everything. What is outlined above is essentially it when it comes to any concrete privacy protections – stuck over two decades in the past. Privacy isn't what it used to be, and the legal protections have not updated with the times. Even "Brandeis and Warren worried that changes in technology as well as law were altering the nature of privacy" (Rosen, 2000, p. 6-7) back in their essay for the *Harvard Law Review* in 1890 -- "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops'" (Rosen, 2000, p. 6-7). Technological developments and changes in social norms are happening at breakneck speed, opening "new and intensified challenges to the scope of privacy rights. In each area, new questions and issues arose to challenge these privacy rights" (Bartee, 2006, p. 265). These challenges have to be met, either proactively or at the very least reactively, as cases come before the courts.

***She said what? I can't believe he took a picture of that – Privacy Present***

An excerpt from <u>*The Unwanted Gaze – The Destruction of Privacy in America*</u> by Jeffrey Rosen (2000):

> At the beginning of the twenty-first century, new technologies of communication have increased the danger that intimate personal information originally disclosed to our friends and colleagues may be exposed to – and misinterpreted by – a less understanding audience. For as thinking and writing increasingly take place in

> cyberspace, the part of our life that can be monitored and searched has vastly expanded. E-mail, even after it is ostensibly deleted, becomes a permanent record that can be resurrected by employers or prosecutors at any point in the future. On the Internet, every Web site we visit, every store we browse in, every magazine we skim, and the amount of time we spend skimming it, create electronic footprints that increasingly can be traced back to us, revealing detailed patterns about our tastes, preferences, and intimate thoughts. …When intimate personal information circulated among a small group of people who know us well, its significance can be weighted against other aspects of our personality and character. By contrast, when intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences. (7-9)

That is the essence of the privacy debate in today's technological realm. The development of social networks and blogging have lead to more and more of ourselves being on display for others to see, in most cases willingly. Yet what about the times when your purchases or Internet habits are tracked unknowingly or information is shared without your consent? Consider the following:

- A loved one is involved in a fatal accident. Days later, crime scene photos showing the lifeless body of your loved one are circulating via e-mail, going "viral"
- You're a young teenage girl, testing the limits to define yourself physically, emotionally and sexually as you experience puberty. As a treat for your significant other, you send him some risqué cell phone photos of you in the new lingerie you just bought. He shows them to his buddy who proceeds to forward them to everyone on the team, who forward them to their friends, and soon, everyone in school knows "Victoria's secret"
- You are a contestant in a national beauty pageant. You've worked hard to develop your image as a beautiful, poised, confident young woman. You wake up one morning to find photos from your MySpace page on the front page of the paper. Someone who you thought was a friend leaked the pictures to the media. You are now forced to explain your private actions with friends in a public forum. Worse yet, since the photos aren't exactly "pageant friendly," you lose your crown

All these cases have actually happened, and we will attempt to address them and others here, with particular attention to how (if possible) the incident could have been avoided and what can be done once the privacy wall has been breached.

*Life after death/Death Remembered*

The first incident is the real life story of the Catsouras family in Orange County, CA. Their 18-year-old daughter Nikki was killed in an automobile accident on Halloween day in 2006. "The accident was so gruesome the coroner wouldn't allow her

parents, Christos and Lesli Catsouras, to identify their daughter's body" (Bennett, 2009, p. 38-40). Yet, nine photos of the accident scene, including one where "her nearly decapitated head is drooping out the shattered window of her father's Porsche" (Bennett, 2009, p. 38-40) are making the viral rounds thanks to a pair of California Highway Patrol officers.

Three months after filing a formal complaint over the photos' release, the family received an apology from the California Highway Patrol. Yet, an apology doesn't prevent the spread of the images around the Internet. The family hired a lawyer and enlisted the services of Reputation Defender, a company that "works to remove malicious content from the Web" (Bennett, 2009, p. 38-40). The most they could do was issue cease-and-desist letters to the sites where the photos appeared and try to implement coding to make the images harder to find via a search engine. Neither approach proved to be very successful – "the family has no legal basis to compel Web sites to remove the photos, and no amount of programming magic could keep them from spreading to new sites" (Bennett, 2009, p. 38-40).

The Catsouras family filed suit against the CHP, with charges including negligence, privacy invasion and infliction of emotional harm. The case was dismissed in 2008, with the judge citing that privacy rights don't extend to the deceased (Bennett, 2009, p. 38-40). The case is on appeal, referencing in particular the 2004 case of Vince Foster, where the Supreme Court "ruled that the government could deny Freedom of Information Act requests for the photos based on a family's right to survivor privacy" (Bennett, 2009, p. 38-40).

The broader issue is how the laws have not caught up with the technology that made the spread of the images so easy. Section 230 of the Communications Decency Act, passed in 1996, gave Web sites immunity from liability for the conduct of individuals on their site, "under the rationale that companies like AOL shouldn't be responsible for the actions of each user" (Bennett, 2009, p. 38-40). Victims are left to try to take action against the specific individuals responsible for the content, a difficult task in the age of anonymous postings. Even if the person responsible is tracked down, odds are the content has already spread beyond their specific site. "We have created a deck that is so stacked against the private individuals who want to protect their name and privacy that you don't even have a fighting chance," says [Michael] Fertik of Reputation Defender (Bennett, 2009, p. 38-40).

*Sexy pictures + text messaging = child porn?*

The second scenario has been played out multiple times in middle schools and high schools across the United States. The phenomenon is popularly known as "sexting" – sending risqué, sexually explicit or nude images via text messaging. In fact, "20 percent of teens said they had sent a sexting message, according to a 2008 study commissioned by the National Campaign to Prevent Teen and Unplanned Pregnancy and Cosmogirl.com" (B., n.d., n.p.). This is typically one of the examples cited when speaking of changing social norms and generational differences in what one considers private, appropriate for sharing or open to everyone.

"When a photo or video is sent to another person, privacy is lost forever. The content can be broadcast to anyone. The original sender has no control once he or she

presses 'send'" (B., n.d., n.p.). Therein typically lies the problem. The sender only intends for the 'sext' to be seen by the original recipient, but they have absolutely zero influence over what that person does once they have the photo. "Explicit photos or videos forwarded from person to person can cause embarrassment for the original sender. Many teens don't realize that once they hit "send," control over who else sees that compromising photo is now completely up to the recipient. You may think you know your friend, boyfriend, or girlfriend, but can you trust them forever?" (B., n.d., n.p.).

Case in point, 18-year-old Floridian Phillip Alpert who "circulat[ed] nude pictures of his girlfriend (which she had sent him), by texting them to his friends, her friends, and her family" (B., n.d., n.p.). The tragic flaw in Alpert's decision -- she was only 16. The innocuous (as innocuous as passing around naked pictures of your girlfriend to friends and family can be) incident becomes a case of child pornography, since technically, he was distributing explicit photos of a minor (B., n.d., n.p.), regardless of the fact that she supplied the images in question in the first place.

Another case of 'sexting gone wrong," one that took a tragic turn, is that of 18-year-old Jesse Logan. The Ohio teen was "mercilessly humiliated after explicit photos she had sexted to a boyfriend ended up circulating among her peers" (B., n.d., n.p.). Unable to escape the embarrassment, harassment and humiliation of having her peers see her in such a compromising situation, she committed suicide.

The National Center for Missing and Exploited Children (NCMEC) has entered the fray, releasing its "Policy Statement on Sexting," one that poses questions including:

- "Was the distribution of the photos done with no malicious regard or desire to harm another, or was it the result of malicious intent by one or more senders?
- What was the intent behind the production of the photos, on a severity scale ranging from a benign reason to supporting a separate and malicious criminal purpose?
- Will prosecution achieve a result which addresses the larger problem of 'sexting' adequately?" (Collier, 2009, n.p.)

So, what does sexually explicit photos of almost legal and barely legal girls have to do with the future of privacy? The issue at hand is not so much the passing around of explicit content featuring teenagers, but how the law is failing to take into account the "changing social practices, mores and technology utilization" (Humbach, 2009, p. 37) of today's online-living world. The definitions and standards used in "governmental policies and initiatives built on past truths and values" are running head-on into "new and unanticipated social phenomena" (Humbach, 2009, p. 37). The laws, as they are being used now, are essentially making child pornographers and sex offenders out of a large portion of America's adolescent and teen population.

Prosecution of cases of 'sexting' and teen autopornography has been shifting away from the umbrella of obscenity – the LAPS test of *Miller v. California (1973)* ("the work, taken as a whole, appeals to the prurient interest, is patently offensive in light of community standards, and lacks serious literary, artistic, political, or scientific value") and moving into the arena of child pornography, where "prosecutors can make a case with little more than proof that the defendant possessed or made of a visual depiction of sexual conduct by a minor" (Humbach, 2009, p. 9-10).

Courts are using the "categorical exclusion" of child pornography materials from First Amendment protection established in the cases of *New York v. Ferber* and *Osborne v. Ohio* as the foundation of many sexting and autopornography rulings, "even though *Ferber* and *Osborne* may not strictly speaking require a conclusion that sexting and other autopornography are unprotected speech" (Humbach, 2009, p. 37).

However, some argue that the "most significant different between teenage autopornography and "traditional" child pornography, … lies in the circumstances under which the two genres are, respectively, produced" (Humbach, 2009, p. 22). The variable at play is the condition of exploitation/coercion/force.

That in mind, the recent case of *Ashcroft v. Free Speech Coalition* is leading some in the legal profession to the notion "that the scope of the categorical exclusion for child pornography [will be] closely aligned with the government objectives that *Ferber* and *Osborne* relied on [the categorical exclusion should be limited to materials that are produced by means of criminal child abuse and exploitation]" (Humbach, 2009, p. 37). A shift if the criteria would mean that sexting teenagers wouldn't "be confronted with the position … that the unprotected category includes any content that visually depicts sexual conduct by minors, *i.e.*, much or most of teen autopornography" (Humbach, 2009, p. 22). The implications of this change in thinking, along with the application of the "current standards of strict scrutiny for content-based regulations" (Humbach, 2009, p. 37) would place sexting and autopornography done by the senders' own actions under the safety of constitutional protection.

This brings to light an interesting point – laws adapting to the changing times. Courts and prosecutors are beginning to realize that the intention of the child pornography laws is not to criminalize most of the teenagers in America for personal behavior done during the process of growing up. In essence, if no crime has been committed, as in autopornography (pictures made by the subject themselves), then it should not be excluded from constitutional protection. While this shift is only in terms of child pornography prosecution, the legal system at large could take their cues from the attempt to adapt to the changing society found in the arena of child pornography prosecution.

*Heavy is the head that wears the crown, especially if it is wearing little else*

The third scenario has happened multiple times in recent years, one such case being that of Miss New Jersey 2007 Amy Polumbo. After being crowned Miss New Jersey, Polumbo and pageant officials received packages containing personal pictures posted online with the threat to make the photos public if she did not give up her crown. Polumbo released the photos herself on the *Today* show, photos described as "normal college pictures" (Giffen, 2008, p. 8-11) showing her in some "unladylike" poses and situations, but nothing explicit or scandalous. Nothing further came from the incident and some even suspected Polumbo staging the whole thing in a publicity stunt. In one of those 'circle of life' twists, Polumbo's pageant platform was raising awareness and education of Internet safety issues to protect children from dangerous situations.

Another pageant incident involved the arguably polarizing Miss California Carrie Prejean. Lost in the debate over her answer during the pageant against the legalization of same-sex marriage is a racy photo controversy that was more likely the reason behind her

losing her title. Following her finishing first runner-up in the Miss USA pageant where she articulated her stance against the legalization of same-sex marriage answering a question from famous Internet gossiper Perez Hilton, news surfaced of the existence of racy photos of the reigning Miss California. Prejean explained the photos were from her modeling swimwear and lingerie and claimed that they were being used to attack her based on her answer to Hilton's question during the pageant (Duke, 2009, n.p.). Prejean was ultimately stripped of her title, with pageant organizers citing numerous breach of contract issues.

A final case to examine is that of Miss Nevada 2007 Katie Rees. Two months following her winning the Miss Nevada crown, photos from June 2004, showing her with friends "goofing off, posing in ways [she] wouldn't want [her] parents to see, doing things [she] wouldn't do off camera, not even thinking about it" (Rees, 2007, n.p.). For Rees, photos from her past saw the light of day on line, thanks to someone she had considered a friend. This case was lost in the news of Tara Conner, the reigning Miss USA who just days before was allowed to keep her crown, given a second chance following reports of underage drinking, drug use and making out with Miss Teen USA.

Again, here is a case of something from someone's past surfacing later in life to cause problems – the same basic argument given for nearly everything people post on the Internet. "Digital information replicates, moves, transmits, and persists. The old joke: "what will survive the nuclear Armageddon?" Answer: cockroaches and Keith Richards. You can now add digital information. What you do, say, post, etc. is not only persistent, it is accessed by and available to the various companies that provide the services. As a result, a number of issues collide: privacy, participation, confidentiality, surveillance, protection, freedom of expression" (Ridley, 2009, n.p.).

*Privacy isn't just about racy photos*

Issues of privacy in today's world are not limited to risqué photos from one's past resurfacing online:

- "As of September 22, there have been 379 data breaches reported by the Identity Theft Resource Center in 2009, affecting more than 13 million records. Companies with data breaches included financial institutions, travel companies, health care operations and schools. … It's a large-scale problem where industry norms of care are arguable not adequate to address the challenges of data security optimally" (Alban, 2009, n.p.).
- According to a survey of "517 US and multinational IT security professionals who work on PCI compliance effort for their companies" released by Imperva and Ponemon Institute (Whitney, 2009, n.p.):
    - "around 55 percent of all businesses acknowledge that they secure credit card information but not Social Security numbers, bank account details, and other personal data … The survey was conducted to determine how many companies are complying with PCI DSS, the Payment Card Industry's Data Security Standard" (Whitney, 2009, n.p.).
    - "71 percent acknowledged not making data security a top initiative, despite the fact that 79 percent of them said they've been hit by one or

more data breaches. In fact, Ponemon and Imperva noted that since the PCI DSS standard was enacted in 2005, the number of breaches and cases of credit card fraud has actually risen" (Whitney, 2009, n.p.).
    - "Cost and lack of resources were the biggest factors cited …" along with organizational priorities (Whitney, 2009, n.p.)
- "Doctors' offices in Tennessee have been … sending patient information, including Social Security numbers and medical histories, [not] to the Tennessee Department of Human Services, [but instead] to Bill Keith, owner of SunRise Solar Inc. in Indiana" (Echegaray, 2009, n.p.)

Then there is the rocky two-year life of Facebook's controversial Beacon service. Released in November 2007, the service was designed to track the user's activities on partner Web sites and report those actions on the user's page to their friends, unless the user opted out. Right from the word go users took issue with the privacy implications of the service. ""Beacon was a disaster, not because it used people's information for commercial marketing purposes," said James Grimmelmann, an associate professor at New York Law School. "It was a disaster because it used people's personal information commercially and then rubbed their faces in it, literally "" (Vijayan, 2009, n.p.). At issue was the information being collected was being used to sell products, not help other users. "It interfered with people's self-presentation, turning them into shills against their will," [Grimmelmann] said" (Vijayan, 2009, n.p.). The Beacon battle is only the latest in a line of issues between Facebook and their users, often over privacy concerns (i.e. – when Facebook altered its terms of service, shifting the ownership of information posted away from the user).

So what does this all mean? We've gone from talking about birth control and the United States Supreme Court to teenagers texting naked pictures of themselves to pageant winners brought down by photos from their past. What on earth does this have to do with the future of privacy? In a word -- everything. It comes down to the fact that it is far from easy to clearly define the concept of privacy. There are a multitude of situations where a breach of privacy for one is no big deal for the next.

Ultimately it comes down to a redefinition of what privacy is and can be done to protect it. Esther Dyson, in an article from *Scientific American*'s September 2008 issue highlighting the future of privacy, postulated that issues masquerading as questions of privacy should often be redefined by what they are actually concerning – typically matters of security, health policy/insurance or self-presentation. With regards to security, Dyson (2008) offers the following analysis:

- "First, in defining some disclosure of information as a breach of privacy, it is useful to distinguish any objective harms arising from the disclosure – fraud, denial of a service, denial of freedom – from any subjective privacy harms, in which the mere knowledge by a second or third party of one's private information is experienced as an injury. In many cases, what is called a breach of privacy is actually a breach of security or a financial harm: if your Social Security number is disclosed and misused … that's not an issue of

privacy; it's an issue of security. As for breaches of *privacy*, the "harm" a person feels is subjective and personal" (p. 51).

- "Second, as the borders between private and public are redrawn, people must retain the right to bear witness. When personal privacy is increasingly limited in a friction-free world of trackable data, the right of individuals to track and report on the activities of powerful organizations, whether governments or big businesses, is key to preserving freedom and to balancing the interests of individuals and institutions" (p. 51).

- "The third point elaborates on the first: in assessing the changes in the expectations people have about privacy, it is important to recognize the granularity of personal control of data. Privacy is not a one-size-fits-all condition: Different people at different times have different preferences about what happens to their personal information and who gets to see it" (p. 51).

To reiterate from the last bullet point – "privacy is not a one-size-fits-all condition." That is what makes the future of privacy such a difficult animal to cage. One man's privacy violation is another's claim to fame. Any efforts to formulate some kind of universal privacy policy are over before they start because consensus is nearly impossible. As for issues of health policy/insurance, Dyson (2008) continues:

> "Security is not the only public issue posing as privacy. Many issues of medical and genetic privacy, for instance, are really issues of money and insurance. … The real issue … is not privacy but rather the business model of the insurance industry in the U.S. … Genetic data seem to present a particularly troubling example of the potential for discrimination. One fear is that insurance companies will soon require genetic tests of applicants -- and will deny insurance to any applicant with a genetic risk" (p. 51-52).

The concern over genetic testing and the privacy of one's personal medical history is a growing concern, especially in the face of the human genome project and continuing advances in genetic testing. Take the increase in the amount of highly personal, unique information that will reside in patients medical records and add to it the increasing use of electronic health records (EHRs). Development of the Nationwide Health Information Network (NHIN) is aimed at creating a "network of networks … establishing electronic formats that will make records of all kinds compatible … easy to transport across networks and across the country" (Rothstein, 2008, p. 66). The secret to the protection of privacy in the old/current paper system is "chaos" – a fragmented system with an individual's records spread across providers in multiple locations over an extensive period of time (Rothstein, 2008, p. 66). To further complicate matters, since every piece of medical information would be available in one central file, those that really don't need your total medical history would still have access to it:

- the orthopedist treating your broken wrist doesn't really need to know about your family's genetic predisposition to a particular cancer

- the insurance company might use your potential for illness based on genetic testing as the basis for charging higher premiums
- employers could discriminate against the potentially-ill, not wanting to hire them so as to not tax the company health plan

So the issue of controlling access to information, in the spirit of Facebook privacy settings, comes into play with regards to your private medical life story. "Rohan Samarajiva defines privacy as "the capacity to explicitly or implicitly negotiate boundary conditions of social relations," and the Internet, properly designed, puts this capacity squarely in the hands of individuals rather than intermediaries" (Rosen, 2000, p. 186). Resolving access issues remains a key piece to resolving the safekeeping of health information.

Finally, with respect to self-presentation, Dyson (2008) offers the following insights:

- "Until recently, privacy for most people was afforded (though not guaranteed) by information friction: Information about what you did in private didn't travel too far unless you were famous or went to extreme lengths to be public about your activities" (p. 54-55).
- "Kids still have a sense of privacy, and they can still be hurt by the opinions of others. It's just that more of them are used to living more of their lives in public than their parents are" (p. 54-55).
- "The issue … is not privacy so much as presentation of self …. People know they cannot control everything others say about them, but they will flock to online-community services that enable them to control how they present themselves online, as well as who can see which of those presentations" (p. 54-55).

Here, Dyson's points resonate more in the realm of social networks and new culture of overshare. A common argument made is that the younger generation today doesn't care about privacy; they share just about everything with just about everyone. Even if that is the case, they still have at least a personal definition of privacy, and it can be violated. This speaks to the need to adjust the definition of privacy to match-up with the current and future direction of society at large. Here again, the idea of being able to control access to your information is what is being broached as they new face of privacy – being able to say who can see what when.

To reiterate the last pair of bullet points addressing young people and their relation to online behaviors and conceptions of privacy, "generation Google" (Solove, 2008, p. 101-102) is altering the very nature of what is considered private and what is considered public. "More and more people have cell phone cameras, digital audio recorders, Web cameras and other recording technologies that readily capture details about their lives" and that in turn means that "nearly anybody can disseminate information around the world" (Solove, 2008, p. 101). Individuals can "spread their ideas everywhere without reliance on publishers, broadcasters or other traditional gatekeepers. But that transformation also creates profound threats to privacy and reputation" (Solove, 2008, p. 102).

However, that technology has created a generational canyon with "high school and college students whose lives virtually revolve around social-networking sites and

blogs" and "…their parents, for whom recollection of the past often remains locked in fading memories or, at best, in books, photographs and videos" on opposite sides (Solove, 2008, p. 101). For those who essentially live their lives as an open book on the web, "the past is preserved on the Internet, potentially forever. And this change raises the question of how much privacy people can expect – or even desire – in an age of ubiquitous networking" (Solove, 2008, p. 101). Sites like JuicyCampus and Don't Date Him Girl don't help the privacy cause any, allowing students to share intimate, sometimes scandalous, not necessarily true details about their classmates.

The social media tools of "generation Google" aren't the only things putting privacy under attack. The everyday collection and use of our personal information by companies and government agencies places our individual privacy at risk (Solove, 2008, p. 103). Databases of our personal information can be amassed and searched, using the information for something beyond its intention. It is this widespread dissemination of our unique, personal information that "diminishes the ability to protect reputation by shaping the image that is presented to others. Reputation plays an important role in society, and preserving private details of one's life is essential to it" (Solove, 2008, p. 103).

One side of the privacy issue praises the chipping away of privacy, theorizing that people might be "less inhibited and more honest" (Solove, 2008, p. 103). The flip side argues that the increasing decrease in privacy will make people more inhibited, since even the smallest past mistake, the fleeting youthful indiscretion will live on in infamy online, never allowing you to "overcome past mistakes" – the "digital baggage" of one's past taking away their ability to "start over" (Solove, 2008, p. 103).

It is in examination Solove's (2008) "Generation Google" that we can find arguably the strongest argument outlining the need to change the way we think about privacy in order to protect it. The notion that "privacy requires total secrecy: once information is revealed to others, it is no longer private … is unsuited to an online world" (Solove, 2008, p. 104). "Generation Google" has a more subtle understanding of what privacy means in today's world:

- "They know that personal information is routinely shared with countless others
- they also know that they leave a trail of data wherever they go
- … recognizes that a person should retain some control over personal information that becomes publicly available" (Solove, 2008, p. 104).

Bottom line, protecting privacy is not a lost cause, but in order to do it successfully, it "requires that we rethink outdated understandings of the concept … privacy does not always involve the sharing of secrets" (Solove, 2008, p. 104).

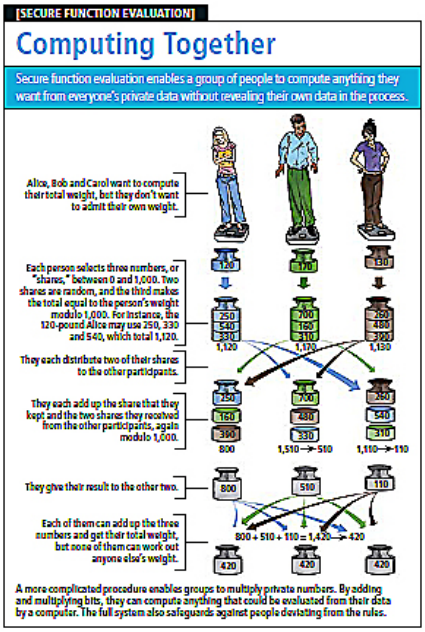
### *It's all fun and games until someone loses their ID – Privacy Protection*

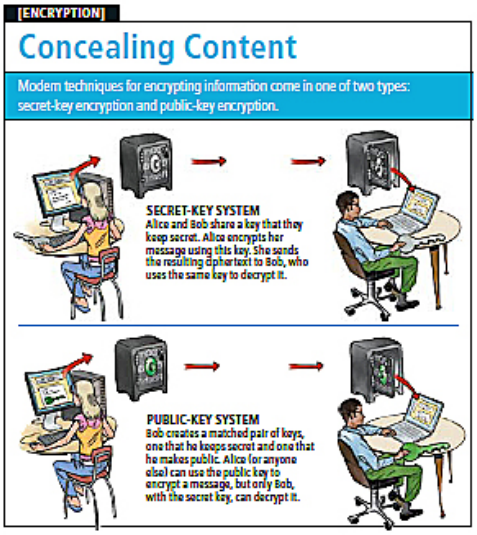
If one is to believe the hypothesis of Dr. Solove, all is not lost; protection of privacy is still possible, even in today's time of social media and overshare culture. As outlined in the Catsouras story, legal avenues are scarce and typically ineffective. That leaves it up to the individual to be proactive is safeguarding their private, personal information. A few guidelines to keep in mind to help fortify your personal information defense:

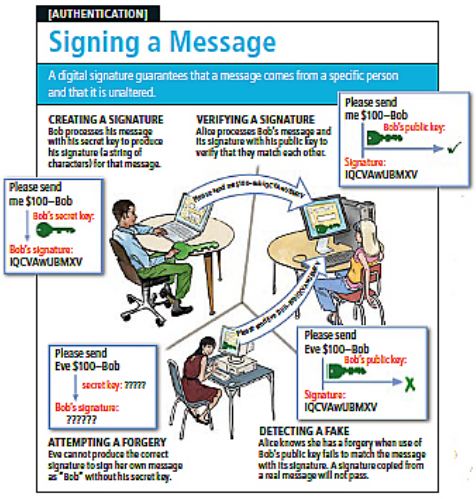
- "Be careful what you share …" – even President Obama touched on the subject in his address to students in September 2009, warning that "whatever you do, it will be pulled up again later somewhere in your life" (Bradley, 2009, n.p.)
- Be mindful of two key fundamentals – "Remember who your friends are, and know that a friend of a friend can be an enemy" (Bradley, 2009, n.p.)
- keep your audience in mind when writing posts, status updates and tweets – "more and more these days, we hear stories of people who have forgotten that their boss is part of their network and have said things online that have gotten them reprimanded, even fired" (leading to the creation of the term 'Facebook fired') (Bradley, 2009, n.p.)
- post with one rule in mind -- "Don't ever post anything online that you aren't comfortable with everyone seeing, because eventually they probably will" (Bradley, 2009, n.p.) – keep your pictures private and watch what you say
- make use of the tools available to you, setting privacy controls where you can
- Safeguard your social security number, as well as other information that can be used to identify you (actual address, school, birthday, etc.)
- Know where your information is going – is it going to be shared with 'trusted partners' (third parties), and if so, how secure are they? (Alban, 2009, n.p.)

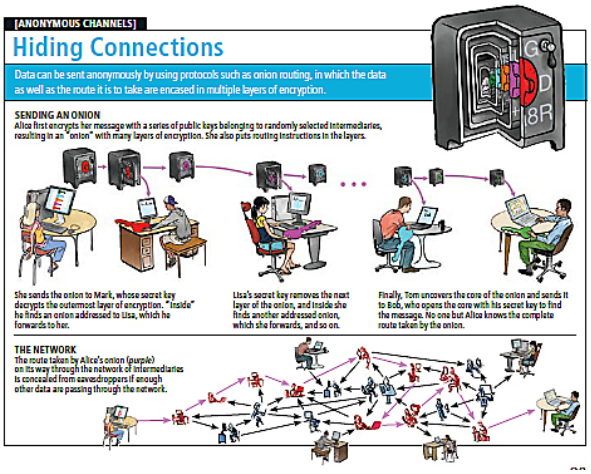
While there may not be many paths of legal recourse when it comes to protecting privacy, and the individual user can only do so much, there are technologies available and in development for the near future that could go a long way toward stronger privacy protection. One of those is the science of cryptography. The available cryptography protocols can be categorized into five overarching categories (each of which has a corresponding diagram from the September 2008 issue of *Scientific American* that illustrates the complexity behind the technology):

1. Secure function evaluation (SFE)
2. Encryption
3. Authentication
4. Anonymous channels
5. Anonymous authorization (a special case of zero-knowledge proof, where a user can prove to another that something is true without revealing what the proof is) (Lysyanskaya, 2008, p. 90-91)



[ANONYMOUS AUTHORIZATION]

## Showing You Belong without Saying Who You Are

A subscriber to a Web site could sign on as a legitimate, registered user without revealing any identifying information by using anonymous authorization. The Web site would not even be able to associate the user with his or her previous visits. Such a protocol is an example of a zero-knowledge proof, in which one party proves a fact without revealing anything about the proof but its validity.

Imagine Alice and Bob play a game with a graph, three colored pens and some paper cups. The graph is a collection of dots, or vertices, connected by lines. Two vertices connected by a line are said to be adjacent. Only some graphs are three-colorable, meaning that three colors suffice to color in all the vertices without coloring any two adjacent vertices the same. Alice will prove to Bob that she has three-colored her graph without giving him any clues about how to three-color it.

The game begins with Bob out of the room. Alice draws six separate copies of the graph. Because she knows how to three-color the graph, she does so with the first copy. For the other five, she uses all of the six possible permutations of her colors. Thus, the six copies of the graph are three-colored in trivially different ways. She chooses one of the six copies at random, places it on the table and covers each vertex with a paper cup. Now Bob returns, and he gets to choose any two adjacent vertices and remove their cups. If the two vertices are the same color, he knows that Alice has been lying and that she has not drawn a valid three-coloring.

They keep repeating the inspection procedure—Bob leaves the room each time while Alice randomly chooses one of the six copies of the graph to place under the cups. From Bob's perspective, if Alice is cheating, she could be showing him many different invalid colorings, and the telltale matching adjacent vertices need not be in the same place on each one. But as he plays enough rounds, the probability that he will catch such cheating approaches 100 percent. Yet at the end of it all, he will not know how Alice has colored the graph. On each round, the two colors he sees on the chosen vertices are random; he might as well have picked the colors himself.

For any statement that has a reasonably short proof (such as "I have the credentials showing that I am an authorized user and over 18"), one can concoct a version of this game that would prove the statement without disclosing any extra information (such as "I am Alice" or "I am user #4790561").

(Lysyanskaya, 2008, p. 90-94)

In addition to the technology of cryptography, developments in the arena of biometrics -- the automated recognition of people via distinctive anatomical and behavioral traits -- are working toward making the future safe for privacy.

" [B]iometric traits are profoundly more difficult to forge, copy, share misplace or guess. … Biometric systems require traits with two basic features: they must be unique for each person, and they must not change significantly with time" (Jain & Pankanti, 2008, p. 78). Three of the most popular traits used in biometric systems are fingerprints, face and iris.

- Fingerprints have been used for over 100 years in law enforcement as a way to identify individuals. Sensors and readers are cheap and compact now, making it easier to take prints as a form of identification. The drawback to the smaller sensors is higher error rates since only a portion of the print is actually read (Jain & Pankanti, 2008, p. 79-80).
- Using the face as the key for a biometric system makes use of the ubiquitous cameras built-in to our computers and cell phones, enabling more areas of to be protected. The drawback is high accuracy only when the image is taken in a controlled environment – same light, angle toward camera, no facial expression (Jain & Pankanti, 2008, p. 80).
- Use of the iris is often favored given its high accuracy and speed. The iris is scanned and the identification is "done by comparing a person's bit sequence to the sequences in a database" (Jain & Pankanti, 2008, p. 80-81). The drawback is using the iris is problematic, since the system depends on "algorithms that represent the random patters in the iris as a sequence of bits – no known human experts can determine whether or not two iris images match" (Jain & Pankanti, 2008, p. 81).

On the surface, biometric security seems like the ideal solution – no passwords to forget, nothing to hack, no PIN to memorize and the key to unlock the security is something unique to each person and is with them always. Yet, the dirty little secret of biometric systems is the entire process is based on the concept of the "imperfect match" (Jain & Pankanti, 2008, p. 81). Systems have to make the call to accept or reject authorization based on how closely what is presented matches what is on file. Depending on the threshold of the system, the errors of "false accept" and "false reject" (Jain & Pankanti, 2008, p. 81) undermine the effectiveness of the protection. The possible solution being employed is reading multiple biometric traits – scanning all ten prints instead of just one; using the prints, the face and the iris in tandem to make the identification.

The use of such personal and unique traits as identifiers raises the privacy red flags. With such a large collection of data, the concern over "who owns the data -- the individual or the service providers" (Jain & Pankanti, 2008, p. 81) is front and center on people's minds. In addition to ownership, the ever-present possibility of misuse of the data or a purpose beyond its original intent raises eyebrows when it comes to using biometric systems.

"Biometric systems of the future will probably operate unobtrusively, capturing biometric traits without the active involvement of the user. Such stealth further confounds the privacy issue" (Jain & Pankanti, 2008, p. 81). The privacy issue is so nuanced, chock-full of shades of grey that even the solutions have problems.

### *Private by Default & Send in the Experts – Privacy Future*

So far, privacy concerns of today appear to center around the unauthorized release and unintended viewing of private, often risqué images that were never meant for the bright spotlight of the public eye. Since this is a futures work, it pays to examine what the movers and shakers in the privacy business believe will comprise the next wave of privacy concerns.

Robert Ellis Smith, publisher of Privacy Journal (http://www.privacyjournal.net/), the oldest privacy publication, sees issues with surveillance and misuse of personal information as major privacy issues of the future, listing "camera surveillance in city streets; behavioral advertising online including the use of search engine data and social networking conversations as the source of data for target marketing and trends toward a national ID card" (personal communication, October 8, 2009). He added, "I have been impressed and disappointed that more Americans are not offended by images of the private residences on [Google] Street View. In Canada, Europe and elsewhere, citizens have been offended" (personal communication, October 8, 2009).

Smith also sees a needed adjustment in how privacy is viewed while agreeing with previous literature on the complexity of privacy:

> Privacy has many dimensions, not simply protecting personal information on the Internet. Those aspects of privacy are alive and well. And in the area of behavioral advertising, Congress is moving ahead with regulatory legislation. Apparently many Americans do not think privacy is dead and that they should simply adjust to a new reality. (personal communication, October 8, 2009)

Bruce Schneier, Chief Security Technology Officer of BT, author and security technologist (http://www.schneier.com/) addressed the issues of information control and law lagging behind the technology in comments he shared:

> We've lost the control of data on some of the computers we own, and we've lost control of our data in the cloud. We're not going to stop using Facebook and Twitter just because they're not going to delete our data when we ask them to, and we're not going to stop using Kindles and iPhones because they may delete our data when we don't want them to. … This loss of control … isn't a technological problem; it's a legal problem. The courts need to recognize that in the information age, virtual privacy and physical privacy don't have the same boundaries. We should be able to control our own data, regardless of where it is stored." (personal communication, September 30, 2009)

And finally, Beth Givens, founder and director of the Privacy Rights Clearinghouse, shared in an interview a pair of issues she sees becoming major privacy issues in the near future:

> Well, I think there are a couple of issues that are behind the scenes right now … that people are going to find in the not too distant future that they're things they are concerned about and one is location privacy. I think most people know that their cell phones, for example ... are able to locate them in an emergency ... that [your] cell phone can be used to locate you. And of course GPS locators in cars ... it's really kind of an up and coming technology; more and more people are using these locational devices but of course there's a huge privacy issue there: who holds that data? how long do they hold on to it? could law enforcement gain access to it if you were ... considered to be part of a crime, a suspect? could the divorce attorney go for it and find out that you were where you said you weren't at 2 AM the other night? … huge privacy issues [and] we haven't even started looking at it. They always say technology goes faster than the laws that protect us ... [and] in this day and age, the laws are way back in the 1970s and 80s unfortunately and we've got new century technologies that are moving ahead at the speed of light ....
>
> [The second is] something called tethered devices ... more and more of these devices ... I'm going to use the Kindle, Amazon's reading machine, the Kindle, is an example of something that you buy, but those books ... in a sense, you kind of rent them.
>
> There was a good example of actually Amazon going in without the consent of the individuals who [owned] these Kindles and actually electronically removing a couple of the books that were there stored on the Kindle ... but without telling them ... they essentially zapped these Kindles, wireless, removed the books. It's a huge irony, but one of the books was George Orwell's 1984 .... So that's an example of a couple of issues ... that I think we're going to be seeing more of as big privacy issues in the very near future." (interview, October 12, 2009)

Our consulted experts touched on a range of issues, so let's quickly recap:

- Camera surveillance on city streets; behavioral advertising online and the movement toward a national ID card are issues Smith has his eye on as likely privacy battles
- Schneier is stressing the need for control over our information as well as the need for the courts to catch up with privacy in the virtual world
- Givens feels that locational privacy and tethered devices will be hot button issues of privacy in the future

By now you have to be questioning the logic of the path we have travelled to get here. From birth control to naked pictures of teens to biometrics to locational privacy, what in the name of all things private does this have to do with the future of privacy? In a word – everything.

The issue of privacy is by no means an easy one to define. What is one person's invasion of privacy is another's opportunity for fame and fortune. Technology is lapping the current action plans (aka legal and structural/systemic privacy protections) in place to handle privacy concerns. The technological development isn't going to slow down any time soon, and that is only going to leave loopholes, grey areas and key problems unaddressed. Uncertainty with regard to ownership of the information and who ultimately has control over it are major points that will need to be addressed as the nature of privacy shifts from keeping secrets to maintaining control.

What role the legal system in general, and the Constitution specifically (since the right to privacy is constitutional), plays in addressing those issues depends primarily upon one's doctrine of constitutional interpretation, according to Associate Professor Scott Gaylord of the Elon University School of Law –

> "Is the Constitution a fixed document establishing general parameters for essential structural and procedural safeguards/rights or is it a 'living, breathing' document, the meaning of which should alter as times change? One's view of that may, in turn, be influenced by how one views the role of the legislature. If the Constitution is silent on an issue, should the legislature be allowed to experiment and respond to the changes you identify or does the Constitution preclude such majoritarian control? If the latter, then how should the Court decide when to 'constitutionalize' an area of law and remove it from the prerogative of state and federal legislatures?" (personal communication, December 3, 2009)

Largely, issues of privacy are addressed in a reactive fashion (in response to a specific question) as opposed to a proactive fashion (anticipating potential questions and planning for them). The legal path to a right of privacy outlined in "Privacy Past" shows the at times glacial evolution of what we now call the "constitutional right of privacy" – a mash-up of five amendments, reading in between the lines to see the hidden privacy right. In each instance, it took a specific incident to spur action.

Furthermore, there is confusion as to what 'privacy' actually means -- if we don't know what it is, how can we effectively protect it? Is it stuck in the early concept of

'property privacy' or is it now in the realm of bodily, personal privacy found in *Griswold*? Does it need to move toward the premise of control over one's information, being able to dictate who sees what when? Is it all of the above plus something not even imagined yet?

It appears to be that the redefinition of privacy as control over your own information is gaining traction as the possible operating concept of privacy in the technological future. "In cyberspace, the greatest threat to privacy comes not from nosy employers and neighbors but from the electronic footprints that make it possible to monitor and trace nearly everything we read, write, browse, and buy" (Rosen, 2000, p. 163). It is controlling access to those electronic footprints that is the likely battleground in the future of privacy.

In a more unconventional notion, "… David Brin in *The Transparent Society* argues [at issue isn't] privacy but access to personal information. Rather than trying in vain to resist a world where ubiquitous video camera mean that our lives are increasingly subject to public scrutiny, … [we] should focus instead on ensuring that all citizens have access to one another's videotapes" (Rosen, 2000, p. 209). Instead of fighting vigorously to keep people from seeing our 'videotape,' privacy should be taken out of the equation all together by opening up everyone's 'videotape' to everyone else. At best it's an utopian ideal – a world where no one cared what others knew or thought about them – one that is not likely to take hold any time soon.

An online diary service based in Toronto may have hit on the answer to the future of privacy and how to handle concerns over protecting it. The service, called Penzu, is an online journaling interface that's private by default. Every entry made on the site automatically has private as the default setting. Users essentially have to opt-in to sharing their work, which they can do via e-mail or a public link to allow comments. This may wind up being the key to saving the future of privacy. Instead of trying to craft a privacy standard that covers every permutation of privacy – an impossible task given that privacy is not a unisex, one-size-fits-all issue – unilaterally shut the door from the beginning. Opt-in sharing may be the magic elixir that cures all privacy ills. Instead of users trying to put the genie back in the bottle by increasing the privacy settings and preferences, users get to control their information, control where and when the genie gets to come out and play.

Jeffrey Rosen (2000) in his book *The Unwanted Gaze*, frames the fate of privacy in terms of societal forces:

> The future of privacy will be determined not by the inherent nature of the Internet, but by social choices about how much privacy we as a society think it is reasonable to demand. And failure to choose means that the slow erosion of protections for private papers and personal information that began at the beginning of the twentieth century will be consummated in the twenty-first century rather than stopped short. Will we be passive in the face of technological determinism, or do we have the vision to insist on rebuilding the privacy we have lost? (p. 195)

This is the dilemma that we must face if we want to ensure there is a future of privacy. Our conception of privacy needs to adapt to the changing world around us to

include the notion of control over one's personal information. Legal protections need to evolve to keep pace with the advancing technological developments, minimizing (and hopefully eliminating) the loopholes that can be exploited leading to violations of privacy. People also need to take an active role in protecting their privacy, making use of the technologies at hand to encrypt, block and limit access to their personal information. Ultimately, the argument can be made that the right of privacy is a constitutional right, a right that needs to evolve to encompass the changing nature of society, a right that we need to exercise before 'privacy right' becomes 'privacy lost.'