

©Stephen Morris  
Information Warfare  
April 2008

***Individual Privacy Rights:  
The US and EU in Comparative Perspective***

In every corner of the Western world, writers proclaim "privacy" as a supremely important human good, as a value somehow at the core of what makes life worth living. Many others have since agreed that privacy is somehow fundamental to our "personhood." It is a commonplace, moreover, that our privacy is menaced by the evolution of modern society, with its burgeoning technologies of surveillance and inquiry. Commentators paint this menace in very dark colors: Invasions of our privacy are said to portend a society of "horror," to "injure [us] in [our] very humanity,"<sup>1</sup> or even to threaten totalitarianism, and the establishment of law protecting privacy is accordingly declared to be a matter of fundamental rights. It is the rare privacy advocate who resists citing Orwell when describing these dangers. At the same time, honest advocates of privacy protections admit that the concept of privacy is increasingly nebulous. In particular, the sense of what must be kept "private," of what must be hidden before the eyes of others, differs widely from society to society.

This paper will analyze the current public policy in the US toward individual privacy, as compared to the traditions of Europe. As private citizens in the US, several laws and regulations are in place to protect privacy, but the question remains as to how effective these mechanisms are. Tracing the development of individual privacy laws, I will argue that a "sectoral model" has been created by policymakers for reasons to be detailed in the essay and that enforcement mechanisms widely differ. Current privacy regulations and enforcement mechanisms generally address one specific sector. For example, HIPAA addresses health information, while FERPA addresses educational information. In understanding the roots of such an approach to creating policy, I will unveil both the limitations and strengths of current US laws by comparing it to the European Union privacy regulations, which differ in tone and tenor.

In fact, we are in the midst of significant privacy conflicts between the United States and the countries of Western Europe - conflicts that reflect unmistakable differences in sensibilities about what ought to be kept "private." But it is not just a matter of the boorish American lack of privacy etiquette. It is also a matter of American law. Continental law is avidly protective of many kinds of "privacy" in many realms of life, whether the issue is consumer data, credit reporting, workplace privacy, discovery in civil litigation, the dissemination of nude images on the Internet, or shielding criminal offenders from public exposure. To people accustomed to the continental way of doing things, American law seems to tolerate relentless violations of privacy in all these areas of law.

These are clashes in attitude that go well beyond the occasional social misunderstanding. In fact, they have provoked some tense and costly transatlantic legal and trade battles over the last decade and a half. Thus, the European Union and the United States slid into a major trade conflict over the protection of consumer data in the 1990s, only problematically resolved by a 2000 "safe harbor" agreement.<sup>2</sup> Europeans<sup>3</sup> still complain that Americans do not accept the importance of protecting consumer privacy.<sup>4</sup> Those tensions have only grown in the aftermath of 9/11.

But it is not just that Europeans resent and distrust the American approach to privacy: The reverse is also true. Americans can be just as obsessively attached to their "privacy" as Europeans, sometimes defending it by resort to firearms. As for American law, it too is obsessed with privacy. Indeed, some of the most violently controversial American social issues are conceived of as privacy matters.

### *Privacy Rights in Trans-Atlantic Context*

Continental privacy protections are, at their core, a form of protection of a right to respect and personal dignity. The core continental privacy rights are rights to one's image, name, and reputation, and what Germans call the right to informational self-determination - the right to control the sorts of information disclosed about oneself.<sup>4</sup> These are closely linked forms of the same basic right: They are all rights to control your public image - rights to guarantee that people see you the way you want to be seen. They are, as it were, rights to be shielded against unwanted public exposure - to be spared embarrassment or humiliation. The prime enemy of our privacy, according to this continental conception, is the media, which always threatens to broadcast unsavory information about us in ways that endanger our public dignity. But of course, this concern does not end with media exposure. Any other agent that gathers and disseminates information can also pose such dangers. In its focus on shielding us from public indignity, the continental conception is typical of the continental legal world much more broadly: in Europe, the protection of personal dignity has been a consuming concern for many generations.<sup>5</sup>

By contrast, America, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home. The prime danger, from the American point of view, is that "the sanctity of [our] home[s]," in the words of a leading nineteenth-century Supreme Court opinion on privacy, will be breached by government actors.<sup>6</sup> American anxieties thus focus comparatively little on the media. Instead, they tend to be anxieties about maintaining a kind of private sovereignty within our own walls.

Such is the contrast that lies at the base of our divergent sensibilities about what counts as a "privacy" violation. On the one hand, we have an Old World in which it seems fundamentally important not to lose public face; on the other, a New World in which it seems fundamentally important to preserve the home as a citadel of individual sovereignty. What Europeans miss in Americans is a sense of the demands of public face; indeed, Europeans have been denouncing American law on that ground since at least 1903.<sup>7</sup> When Americans seem to continental Europeans to violate norms of privacy, it is because they seem to display an embarrassing lack of concern for public dignity - whether the issue is the public indignity inflicted upon Monica Lewinsky by the media, or the self-inflicted indignity of an American who boasts about his salary.

Conversely, when continental Europeans seem to Americans to violate norms of privacy, it is because they seem to show a lack of resistance to invasions of the realm of private sovereignty whose main citadel is the home - whether the issue is wiretapping or registering with the police. The question of public nudity presents the contrast in piquant form. To the continental way of seeing things, what matters is the right to control your public image - and that right may include the right to present yourself proudly nude, if you so choose. To the American mind, by contrast, what matters is sovereignty within one's own home; and people who have shucked the protection

of clothing are like people who have shucked the protection of the walls of their homes, only more so. They are people who have surrendered any "reasonable expectation of privacy."<sup>8</sup>

Americans and Europeans certainly do sometimes arrive at the same conclusions. Nevertheless, they have different starting points and different ultimate understandings of what counts as a just society. American privacy law is a body focused on liberty values, while European law focused on preserving dignity.

### *EU Data Protection Directive*

The European Union Directive on Data Protection reflects the commonly held belief in the EU that, while data processing is beneficial, an individual's "fundamental privacy rights" must be protected in all EU Member States. Further, the Directive ensures that corporations, including both European companies and U.S. multinationals doing business in the EU, do not circumvent the EU's data protection laws by exporting personal data to destinations not subject to EU privacy rules. Many EU Member States have had data protection laws since the 1980s. However, since these laws are generally not as comprehensive as the Directive, most EU countries require new legislation to comply fully with the Directive. According to information released by the European Commission, as of June 2002, twelve Member States have enacted laws or regulations implementing the Directive in full.<sup>9</sup> Despite the Commission's issuance of "reasoned opinions" to Members that have not yet implemented the Directive—the second stage in a formal infringement proceedings<sup>10</sup> under EU law —three Member States still have not enacted implementing legislation.—

The Directive applies to the collection, transmission, and processing of "personal data" within the EU and has three primary components: 1) regulations regarding the collection and handling of personal data; 2) regulations concerning the legitimate processing<sup>11</sup> of personal data; and 3) regulations regarding the exportation of personal data from the EU.— The Directive requires Member States to ensure that their implementing legislation gives individuals a direct right of action for mishandling their personal data. "Personal data" is defined as "any information relating to an identified or identifiable natural person."<sup>12</sup>—

First, with respect to the collection and handling of personal data, Member States must ensure that corporations manage personal data so that it is collected for specified and legitimate purposes and not processed further; relevant and not excessive for the purpose collected; accurate and updated as necessary<sup>13</sup>; and kept in a form that permits identification of data subjects for no longer than necessary.— Moreover, individuals (or "data subjects") must be informed of the identity of the individual in charge of the data (or "data controller"), whether they are required to submit their personal data to the data controller<sup>14</sup>, their right of access to the data, and their right to correct any errors in the data.—

Second, corporations may not process personal data unless the data subject has unambiguously given his or her consent or processing is necessary to legitimate interest pursued by the data controller or a third party, except where the data subject's privacy interests outweigh.— In addition, the data controller must notify the Member State's data protection authority before carrying out any wholly or partly automated processing operation.

Third, personal data may be exported from the EU only if the third country "ensures an adequate<sup>16</sup> level of protection" of such data, or if some exception applies to the particular transfer.— Exceptions to the Directive's transfer restriction include for when the data subject has unambiguously given his consent to the data transfer or the transfer is necessary to protect the

vital interests of the data subject. Most importantly, an EU Member State may authorize the transfer of personal data to a third country that does not, as a matter of law, ensure an adequate level of protection if the data controller can demonstrate the existence and applicability of safeguards sufficient to protect the privacy of the specific export, giving particular regard to contractual clauses that guarantee privacy.

### *US Privacy Protection Laws*

As previously indicated, the US approach to privacy protection is “sectoral” as opposed to the European omnibus approach, illustrated in the Data Directive. Below, I summarize some of the most important privacy regulations in the US by sector.

#### *Privacy Act of 1974*<sup>17</sup>—

This Act is the only federal omnibus Act that protects informational privacy. The Privacy Act applies only to data processing by the federal government and not to state governments or the private sector. The Act obliges federal agencies to collect information to the greatest extent possible directly from the concerned individual, to retain only relevant and necessary information, to maintain adequate and complete records, to provide individuals with rights of access to review and have their records corrected, and to establish safeguards to ensure the security of the information. The Act contains a significant exception in the form of the “routine use exception” that permits federal agencies to transfer information between themselves for what they justify as a “routine use.” Since the Act does not apply to private sector databases, federal agencies have increasingly relied on them.<sup>18</sup>—

#### *The Electronic Communications Privacy Act of 1986 (ECPA)*<sup>19</sup>—

The ECPA requires government officials who wish to intercept or obtain electronic communications—such as email or other information available electronically, such as Internet Service Providers (ISP) logs and public library patron records - to seek and receive permission, known as a “Title III” order, from a federal judge. The ECPA has been amended by the USA PATRIOT Act.

#### *The Privacy Protection Act of 1980*<sup>20</sup>—

Despite its title, this Act serves to protect free speech and First Amendment rights, not privacy in general. The Act prohibits government from searching or seizing any work or materials held by a person intending to disseminate it to the public in some form of public communication (e.g. newspapers, books, broadcasts) without court authorization. There has not been any ruling yet as to whether the Act applies to forms of electronic communication such as message boards.

#### *The Family Educational Rights and Privacy Act (FERPA)*<sup>21</sup>—

This Act, passed in 1974, protects the privacy of student records at all educational institutions receiving federal funding (e.g. universities and colleges.) Educational institutions cannot disclose student records or personal information to third parties without consent, and must grant the students access to such information held by the institution. Students have the right to challenge and amend inaccurate records.

#### *Driver’s Privacy Protection Act*<sup>22</sup>—

This Act of 1994 prohibits the public disclosure of personal information contained in state department of motor vehicle records for marketing purposes, unless drivers expressly consent. The Act was challenged as unconstitutional (Congress interfering in state-jurisdiction), but was upheld by the Supreme Court. Personal information can still be disclosed for many other purposes (e.g. private investigations, toll payment, and identity confirmation) without consent, so the Act, despite its title, only offers limited protection to drivers.

#### *The Right to Financial Privacy Act*<sup>23</sup>

The Right to Financial Privacy Act was designed to protect the confidentiality of personal financial records, but only from government. The Act essentially provides statutory Fourth Amendment protection to bank records (i.e. law enforcement agencies cannot access or seize records without some form of authorization such as a warrant). Furthermore, financial institutions cannot obtain “blanket” consent from customers to release records as a condition of doing business. Customers also have a right to access a record of all disclosures made of their personal information.

#### *The Fair Credit Reporting Act (FCRA)*<sup>24</sup>

Another Act addressing the realm of personal finances is the FCRA. The FCRA was originally passed in 1970, amended in 1996, and most recently amended in 2003. It authorizes the Federal Trade Commission (FTC) to regulate the private sector in the area of credit reporting. Businesses reporting credit (known as Consumer Reporting Agencies) are obligated to report credit information accurately and fairly, to correct any errors in their reports, and to include a consumer’s dispute of their credit record as part of the report. Although the FCRA recognizes the consumer’s right to privacy, and some measures in the FCRA do address privacy (e.g. the consumers have a right to access their records, albeit for a fee), the FCRA is primarily concerned with ensuring credit accuracy. This purpose of the FCRA is compatible, of course, with the overall goal of increasing marketplace efficiency - and consumers, at the end of the day, cannot prevent Consumer Reporting Agencies from forwarding their credit reports to any person with a “legitimate” interest, such as potential employers or insurance companies.

#### *The Financial Modernization Act*<sup>25</sup>

This recent Act (1999), more commonly known as the Gramm-Leach-Bliley Act (GLBA), is the first to attempt some form of privacy regulation in the financial sector, rather than simply restrict government access to financial information or ensure market efficiency, as the Acts above. The Act requires that financial institutions have a privacy policy and that they bring it to their customers’ attention. Although financial institutions are broadly defined (e.g. car dealerships offering leases are included), the legislation fails to set any principles for those policies. Customers are able to opt-out - that is, stipulate to their financial institutions that they do not want their personal information to be shared with other businesses in certain circumstances. Nonetheless, affiliated businesses may share information freely. The Act is administered by the Federal Trade Commission (FTC).

#### *The Identity Theft and Assumption Deterrence Act*<sup>26</sup>

This Act, enacted in 1998, criminalizes the unauthorized use for a felonious purpose of another person’s identity, and provides for penalties of up to fifteen year imprisonment and a

maximum fine of US\$250,000. It establishes that the person whose identity was stolen is a victim and allows this victim to seek restitution (previously, only businesses [e.g. financial institutions], which suffered monetary losses, were considered victims). The Act is administered by the FTC. Note that the Act does not provide protective measures for privacy. Rather, it creates criminal sanctions for invasion of privacy in order to deter identity theft.

#### *The Cable Communications Policy Act*<sup>27</sup>

This Act regulates the cable industry in the US generally, and incorporates several specific privacy measures. Cable companies are not allowed to collect personal information without consent, or to disclose it to third parties, unless the information is necessary for service purposes. Together with the following Act, it is an example of the American piecemeal approach to privacy of personal information.

#### *The Videotape Privacy Protection Act*<sup>28</sup>

This Act was passed due to the controversy surrounding the release of Judge Bork's video rental records during his failed Supreme Court nomination. The Act prohibits video stores from disclosing customer records without their consent. Furthermore, the Act requires video stores to destroy personal information within a year of the date that it is no longer necessary for the purpose for which it was collected. The Act is under review by the US Supreme Court.

#### *The Telephone Consumer Protection Act*<sup>29</sup>

This Act, enacted originally in 1991 and amended since, sets the legislative basis for the Federal Communications Commission (FCC) to establish a "do-not-call" list for telemarketers. Telemarketers are required under the Act to maintain such a list and abide by the wishes of listed consumers not to be called.

#### *The Telecommunications Act of 1996*<sup>30</sup>

Within the Telecommunications Act of 1996, which updated the Communications Act of 1934, are specific privacy measures designed to limit marketing on behalf of telephone companies, based on their ability to access their customers' calling patterns. Telephone companies must obtain express consent from customers to use such data for marketing purposes, although the Act does not state how the consent is to be obtained. The Act is administered by the FCC.

#### *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)*<sup>31</sup>

HIPAA sets out to eliminate "job-lock"—that is, the denial of employment based on medical information. In order to protect personal medical information traveling from healthcare providers and administrators to potential employers, HIPAA establishes privacy measures, which aim to be a minimal standard to which states can add. Personal health information in the hands of healthcare providers, health plans, and healthcare clearinghouses (i.e. data and billing processors, commonly referred to as "covered entities") cannot be disclosed without the patient's express consent. Consent under HIPAA must be obtained prior to treatment, yet it is not required for treatment, payment or other healthcare operations (e.g. delivery of medical equipment to a patient's home). Further, patients have a right to access and amend their information, and a right to know to whom the information has been provided. HIPAA is administered by the Office of

Civil Rights in the Department of Health, which can impose both civil and criminal penalties of up to \$250,000 and 10 year imprisonment.

### *The Children's On-line Privacy Protection Act of 1998 (COPPA)*<sup>32</sup>—

COPPA was passed in 1998 to protect children's personal information from collection and misuse by commercial websites. COPPA requires commercial websites and other online services directed at children 12 and under, or websites which collect information regarding age, to provide parents with notice of their information practices and to obtain parental consent prior to the collection of personal information from the children. The Act further requires such sites to provide parents with the ability to review and correct the information about their children that was collected by such services. COPPA is administered by the FTC, and must be distinguished from several other acts passed in the US in recent years aimed at curbing child pornography, such as the Communications Decency Act of 1996 (CDA); the Child Pornography Prevention Act of 1996 (CPPA); and the Child Online Protection Act of 1998 (COPA).

### *The Right to Privacy?*

The absence of a constitutional right to privacy (particularly in light of its existence in several state constitutions) gives rise to two broad constitutional concerns regarding privacy. The first is that the US sectoral approach will result in various privacy-protecting acts clashing with well-established constitutional rights. As a result, these Acts and their protection of privacy are subject to constitutional review, and may be watered down if not stricken down outright. The second is that the US Constitution with its supporting body of jurisprudence may not provide adequate privacy protection, especially in light of continuing technological development. Privacy advocates fear that many such developments, such as public video surveillance, will, if they come before the courts, be simply ruled to be constitutional and the privacy right not "worthy" of the Constitution's protection in that context.

Discussions of privacy protection in light of the First Amendment exemplify the first broad concern. The constitutional right to free speech is very important to Americans, and any attempt to regulate the content of free speech is highly suspect under the First Amendment. The controversy in the US about freedom of the press and the more generalized freedom of speech is as old as the American colonies, but until recently commercial interests did not presume to invoke the First Amendment guaranty of freedom of speech as covering commercial speech. Over the last thirty years, however, there have been cases in which the private sector has successfully argued that legislation ostensibly protecting privacy imposes an unconstitutional restriction on free speech. Among the Acts attacked were the CDA, COPA and CPPA. All were declared unconstitutional by the courts.<sup>33</sup>—

First Amendment rights are also relevant to privacy protection due to the well received view that the internet is the ultimate First-Amendment enabling technology because it allows anyone, regardless of wealth, status or political clout to share opinions with the world.<sup>34</sup>— The idea that an Orwellian "Big Brother" would be authorized to monitor which websites an individual visits or what messages he or she sends through cyberspace is often contradictory to the American value of free speech.

As an example of the second broad constitutional concern, that the Constitution will ultimately prove to provide inadequate privacy protection, consider the discourse of the privacy protection offered by the Fourth Amendment. The Fourth Amendment protects against unreasonable

searches and seizures by government. Privacy advocates note, of course, that reasonable searches and seizures are permitted. That, in turn,<sup>35</sup> has led the Supreme Court to consider what exactly reasonable expectations of privacy are.— For instance, consider video surveillance of public spaces. Modern video cameras are not static devices with limited image storage on endlessly looping video tapes, but active devices that can be manipulated to trace an individual's movements within the camera zone, and that can communicate with each other to ensure continuous coverage as individuals move from one camera area to another. Furthermore, images can be digitally recorded for posterity. However, the very discussion of expectations in such a context is moot. The Supreme Court has ruled that there are no privacy expectations in public, which is the space covered by video cameras.<sup>36</sup>— Thus, the protection granted by the Fourth Amendment does not extend to such expectations of privacy.

Consider other technological developments, known collectively Global Positioning Systems that can be worn on the person, implanted under the skin, installed in vehicles and in cellular phones, in “black box” devices installed in vehicles, and in Inter-Vehicle Communication Devices. Such technology raises privacy issues, not only with respect to government's use, but also with respect to the private sector and the extent to which employers, for instance, can monitor employees and their use of the “company car” and the “company phone,” or to which marketing firms can mine data accumulated by GPS locators. None of these issues, however, currently falls under Fourth Amendment protection, mainly, again, because these technologies are primarily applied in public spaces.

Finally, there is of course the issue of searches and seizures conducted by new means, such as the development of DNA databases or the execution of “digital” searches.<sup>37</sup>— The Fourth Amendment does not appear to offer effective privacy protection against these new forms of searches, and it appears, again, to have been closely circumscribed outside of the realm of physical privacy. State entities have not been held to the same exacting standard with respect to digital searches as have been applied to physical searches and seizures. Thus, some privacy scholars have concluded that constitutional protection against government misuse of digital searching is minimal.<sup>38</sup>— It is important to remember in this context, moreover, that while constitutional protection may be weak, protection has been, at least until now, provided to members of society primarily under the ECPA, but because courts have had a tendency, particularly post 9/11, to dismiss privacy concerns when national security might be at stake. For decades, the US Supreme Court has struggled to balance law enforcement's legitimate need to capitalize on advances in electronic surveillance technology with an individual's constitutional right to be secure against unreasonable searches and seizures. How this balance will shift in light of present fears of terrorism remains to be seen.

<sup>1</sup> Solove, Daniel J., Marc Rotenberg, Paul M. Schwarz. *Privacy, Information and Technology*, Aspen Publishers, 2006. (paperback version)

<sup>2</sup> Rehder, J. & Collins, E.C., “The Legal Transfer of Employment-Related Data To Outside the European Union: Is It Even Still Possible?,” 39 *International Law* 129 (Spring 2005)

<sup>3</sup> *Ibid.*

<sup>4</sup> Rehder, J., *op. cit.*

<sup>5</sup> *Ibid.*

<sup>6</sup> Solove, Daniel., *op. cit.*

<sup>7</sup> Rehder, J., *op. cit.*

- [8](#) Westin, Alan F., "Social and Political Dimensions of Privacy," *Journal of Social Issues* No. 2 431-53 (2003).
- [9](#) Rehder, J., *op. cit.*
- [10](#) *Ibid.*
- [11](#) Rehder, J., *op. cit.*
- [12](#) *Ibid.*
- [13](#) *Ibid.*
- [14](#) *Ibid.*
- [15](#) *Ibid.*
- [16](#) Rehder, J., *op. cit.*
- [17](#) Available online at [http://epic.org/privacy/laws/privacy\\_act.html](http://epic.org/privacy/laws/privacy_act.html)
- [18](#) Rotenberg, Marc, "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11" (September 28, 2006). Available at SSRN: <http://ssrn.com/abstract=933690>
- [19](#) Available online at <http://www.law.cornell.edu/uscode/18/2510.html>
- [20](#) Available online at <http://www4.law.cornell.edu/uscode/42/2000aa.html>
- [21](#) Available online at <http://www.law.cornell.edu/uscode/20/1232g.html>
- [22](#) Available online at <http://www4.law.cornell.edu/uscode/18/2721.html>
- [23](#) Available online at <http://www.fdic.gov/regulations/laws/rules/6500-2550.html>
- [24](#) Available online at <http://www.law.cornell.edu/uscode/15/1681.html>
- [25](#) Available online at [http://www.law.cornell.edu/uscode/15/usc\\_sup\\_01\\_15\\_10\\_94.html](http://www.law.cornell.edu/uscode/15/usc_sup_01_15_10_94.html)
- [26](#) Available online at <http://www.ftc.gov/os/statutes/itada/itadact.htm>
- [27](#) Available online at <http://www4.law.cornell.edu/uscode/47/551.html>
- [28](#) Available online at [http://assembler.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00002710----000-.html](http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html)
- [29](#) Available online at [http://www.law.cornell.edu/uscode/html/uscode47/usc\\_sec\\_47\\_00000227----000-.html](http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000227----000-.html)
- [30](#) Available online at [http://assembler.law.cornell.edu/uscode/html/uscode47/usc\\_sec\\_47\\_00000609----000-.html](http://assembler.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000609----000-.html)
- [31](#) Available online at <http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf>
- [32](#) Available online at <http://ftc.gov/ogc/coppa.htm>
- [33](#) Solove, *op. cit.*
- [34](#) Ric Simmons, "Technology Enhanced Surveillance by Law Enforcement Officials" (2004) *Public Law & Legal Theory Working Paper Series*, No. 10 [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=539704](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=539704)
- [35](#) *Katz v. United States*, 389 U.S. 347 [http://straylight.law.cornell.edu/supct/html/historics/USSC\\_CR\\_0389\\_0347\\_ZS.html](http://straylight.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html). (1967) [Katz].
- [36](#) Solove, *op. cit.*
- [37](#) Bonnie L Taylor, "Storing DNA Samples of Non-Convicted Persons & The Debate Over DNA Database Expansion" (2003) 20 *Thomas M. Cooley Law Review* 509.
- [38](#) Stephen A. Osher, "Privacy, Computers and the PATRIOT Act: The Fourth Amendment Isn't Dead, But No One Will Insure It" (2002) *Florida Law Review* Vol. 54, <http://www.flr.law.ufl.edu/pdf/july2002/osher.pdf>.