The Sedona Conference Journal

Volume 12 2011

Privacy in the Post-Modern Era—An Unrealized Ideal?

Damon Greer

Recommended Citation: Damon Greer, *Privacy in the Post-Modern Era—An Unrealized Ideal*, 12 SEDONA CONF. J. 189 (2011).

PRIVACY IN THE POST-MODERN ERA – AN UNREALIZED IDEAL?

*Damon Greer,**
U.S. Department of Commerce
Washington, DC

I am not only retired from all public employments, but am retiring within myself, and shall be able to view the solitary walk and tread the paths ofprivate life with heartfelt satisfaction.

— George Washington,
Letter to the Marquis de Lafayette, 1784

1. INTRODUCTION

Many in the legal community are acquainted with the long, relentless journey data protection law has taken in the European Union since the 1950 Council of Europe Convention for the Protection of Human Rights & Fundamental Freedoms (Article 8). Earlier, the United Nations published the Universal Declaration of Human Rights on December 10, 1948. Article 12 states: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."*

Privacy as a "fundamental human right" emerged conceptually in Europe following the Second World War amid the revelations of how people were identified, persecuted, and then killed systematically by the Nazi regime. Evocative of the role personal data played in the "Final Solution" is the opening scene of "Schindler's List" at the train station in Krakow. The camera portrays the regime's relentless efficiency in collecting data from arriving Jews who were ordered to report to Krakow where they were forced into the ghetto. The first word spoken in the film is "name." Later in the film, the ubiquitous "list makers" appear whenever a transport was being organized, a culling out of the sick and feeble was ordered, or when people were sent away for "special treatment." Later, in the film, "The Lives of Others," the Stasi – the Ministry for State Security – works assiduously to spy on Eastern Germany's citizens, a surveillance program built on paranoia and power that continue up to the collapse of the German Democratic Republic. The film's final irony is underscored by the principal investigator's new job under a reunited Germany – that of a postman.

Today, the European Union's cornerstone of its legal framework is the Data Protection Directive (95/46/EC), which passed in 1995 and entered into force on October 25, 1998. EU member states were required to enact national data protection laws that

* The views expressed herein belong to the author and do not represent those of the Department of Commerce or the administration.

implemented the directive and established independent data protection authorities to enforce them. EU enlargement has expanded to number 27 countries today, and together with three European Economic Area (EEA) members—Norway, Iceland, and Liechtenstein—30 countries are now bound to the directive's provisions and participate in the Article 29 Working Party's regular deliberations and consultations regarding the impact new technological advances and innovation have on protecting member states' citizens.

In the past ten years, many influence leaders in both the public and private sectors have called for a global framework for protecting personal data and privacy that would adapt to the borderless character of data flows prevalent in the world today.[1] The International Conference of Data Protection and Privacy Commissioners, a group of data protection officials from EU member states and other countries that have a formal data protection regime embodied in law have promulgated a series of proposals that would establish a common global legal framework based on common privacy principles. The first attempt at establishing transnational guidelines was the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the OECD Council on September 23, 1980.[2] Current efforts to have a harmonized global privacy framework adopted date back to the Montreaux Convention in 2005 – the 27th International Conference of Data Protection and Privacy Commissioners, later iterations of the same conference up to the 31st International Conference of Data Protection and Privacy Commissioners in Madrid last November where the so-called Spanish Proposal – International Standards on the Protection of Personal Data and Privacy – was released.[3] The International Conference again called for a United Nations convention to develop a treaty or similar instrument that would provide legal certainty for data protection and privacy worldwide.

Nonetheless, the nature and character of data flows has dramatically shifted to a new, more dynamic paradigm—data access—whereby information is accessed globally via Web 2.0 technologies from and by anyone with the authority to do so. In addition, social network service providers, i.e., Facebook, LinkedIn, MySpace, etc., empower users to manage their personal data with enhanced privacy controls heretofore absent or misunderstood previously. Still, the struggle between the two principal camps—the European Union and the United States—remains and the debate continues. This conflict was recently highlighted in an article written by Adam Liptak in *The New York Times*.[4] Is it privacy or data protection? Is it a fundamental human right or a consumer's right? The debate continues and the methods designed to protect citizens' privacy are embodied in data protection laws which serve as the basis for competing legal frameworks. Today, more than 50 nations have enacted data protection laws designed to protect privacy. To the extent they are effective remains unknown but the most recognized framework – that of the European Union is undergoing a review of its foundational law, the Directive 95/46/EC, commonly known as the data protection directive. What, if any, changes will be made remains unknown but pronouncements from EU data protection officials across the spectrum indicate it is indeed time for a change. In an era of global Internet traffic flows that recognize no national boundaries, is privacy truly an unrealistic ideal or may it be strengthened with new, innovative approaches to control that empower the digital citizenry in the future?

---

1 Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects, Computer Law and Security Review*, 25 COMPUTER LAW & SECURITY REVIEW, 307-17 (2009).

2 *See* the Directorate of Science and Technology, OECD Guidelines on the Protection of Privacy and Transborder Data Flows, Sept. 23, 1980, *available at* http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

3 Agencia Española de Protecccción de Datos. International Standards on the Protection of Personal Data and Privacy, Nov. 5, 2009, *available at* https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.

4 Adam Liptak, *When American and European Ideas of Privacy Collide,* THE NEW YORK TIMES, Feb. 26, 2010.

Since 2009, in the United States, online privacy has received heightened scrutiny, enhanced enforcement from the Federal Trade Commission, and deliberations in the Congress to develop and enact comprehensive online privacy legislation that would provide protection to the consumer who uses the Internet whether for social networking, online commercial transactions, information acquisition, or shopping. During 2010, the FTC has held a series of roundtable discussions on privacy that, inter alia, have examined the prevalent regulatory model by which it exercises its enforcement authority under Section 5 of the FTC Act of 1914 – notice and choice. The commission expects to issue its findings from the year-long review this autumn. In remarks delivered at New York University in October 2009, David Vladeck, director of FTC's Bureau of Consumer Protection outlined the agency's approach to protecting privacy noting that the Commission's goal has remained constant for more than 10 years: "To protect consumers' personal information and to ensure that consumers have confidence to take advantage of the many benefits offered by the ever-changing marketplace….the strategies have evolved to adapt to changing technologies and business practices."[5] He noted that new technologies have raised privacy concerns not readily resolved by existing privacy frameworks and that both the consumer and the enterprise now must be alert to understanding the technologies and while being transparent in how privacy practices, data use, and marketing impact how privacy is assured. Similarly, in testimony before the Senate Commerce Committee in late July, FTC chairman Jon Leibowitz noted that three principles emerged from the privacy roundtables: 1) Privacy by design, 2) Simplified controls, including the potential for a "do not track" mechanism in a Web browser, and 3) More transparency about how private information would be used. Generally, opt-in would be preferred over opt-out in the use of private data coupled with clear notice. Testifying at the same hearing, FCC chairman Genachowski noted "the privacy issues discussed here are not only a fundamental moral issue. To get the economic effects of broadband, people need to be confident that the Internet is a trustworthy place."[6]

II. EVOLUTION OF THE PRIVACY DEBATE IN THE UNITED STATES

The Constitution of the United States of America ratified in 1789 does not explicitly mention or refer to a "right of privacy." There are those that believe that privacy is the intent behind the Bill of Rights, the first 10 amendments to the Constitution and that the 4th Amendment – Search and Seizure establishes the implicit right to privacy. Supreme Court cases solidified that there is a "reasonable expectation to privacy and that privacy rests in the person not in the person's property."

The Fourth Amendment – Search and Seizure

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Historically, the concept (right of privacy) first appeared in 1890 in a *Harvard Law Review* article by Samuel Warren and Louis Brandeis. They used the term in proposing a new tort – the invasion of privacy – in their complaint about how the PRESS was printing lurid accounts of the social activities of the Warrens, a prominent Boston family.

5 David C. Vladeck, Director, FTC Bureau of Consumer Protection, "Promoting Consumer Privacy: Accountability and Transparency in the Modern World," Speech given at New York University (Oct. 2, 2009).
6 Alex Howard, "Can New Online Privacy Laws be Balanced with Innovation and Social Benefit?" *available at* http://radar.oreilly.com, Aug. 6, 2010.

They distinguished it from injury to reputation on grounds that invasion of privacy was a deeper harm, one that damaged a person's sense of their own *uniqueness*, *independence*, *integrity*, and *dignity*, making the astonishing claim (for 1890) that privacy was a personal, not a property, right.[7]

In 1965, the Supreme Court, in *Griswold v. Connecticut,* 381 U.S. 479 (1965), established the "penumbra" constitutional right of privacy. Justice William O. Douglas wrote:

> "Previous cases suggest that the specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that give them substance. Various guarantees create zones of privacy, such as the First Amendment right of association, the Fourth Amendment right to be secure in one's person, house, papers, and effects, the Fifth Amendment right not to surrender anything to one's detriment, and the Ninth Amendment right to not deny or disparage any right retained by the people. These cases press for recognition of the penumbral rights of privacy and repose." (Justice Douglas, for the majority with Goldberg, Warren, & Brennan also concurring)

Katz v. U.S., 389 U.S. 347 (1967), is recognized as the definitive case that signaled the most definitive shift in what constitutes privacy. It shifted the definition of privacy from being *place-based to being person-based* (heretofore, conceptions of privacy derived from the "property" concept of life, liberty, and property; and…from the Common Law *trespass doctrine* that 'every man's home is his castle').

Additionally, *Katz v. U.S.* balanced the interest in protecting individuals from government intrusion with the interest in protecting society from criminals and created a two-prong test for "reasonable expectation" based on this balance. The "reasonable expectation test is based on:

- **Subjective privacy**, i.e., whether the person exhibited a personal expectation to be left alone from governmental intrusion, and

- **Objective privacy**, i.e., whether the personal expectation is one that society is prepared to recognize as reasonable and several areas have already been determined to be beyond what society is willing to recognize: items in plain view, hearing, smell, and touch; open fields; public places, and abandoned property.[8]

Collectively, these Supreme Court decisions serve as the fundamental basis for establishing constitutionally the "right to privacy." These settled precedents and contemporaneous federal legislation discussed below form the framework along with their civil and criminal enforcement provisions for privacy protection in the United States.

The debate continues in the 111th Congress. Online privacy is the current focus of the debate and legislation protecting consumers' privacy whilst logged into the Internet has been drafted to provide protections and to provide legal certainty for both the business community and the public. Unlike the European Union where personal data is "owned" by the data subject or citizen, data ownership in the United States rests with the entity that

7 Thomas O'Connor, Professor of Law, Lecture Notes on Criminal Procedure, Fall 2001, North Carolina Wesleyan College, Rocky Mount, N.C.
8 *Id.*

possesses it. Legislation under consideration would alter that model and shift "ownership" to the individual by according control over its use from the data holder to the data subject or consumer. Both of the leading bills in the House of Representatives (H.R. 5777) sponsored by Representative Bobby Rush and introduced on July 19, 2010, and Richard Boucher's draft online privacy bill received criticized by both industry and privacy advocacy groups. Subsequent discussions between the two indicate that a combined bill may be introduced in the fall.

The U.S. Senate Committee on Commerce, Science, and Transportation held a full committee hearing on July 27, 2010, whose topic was Consumer Online Privacy. Committee members' principal concerns were (1) individual profiles built by advertisers and web-companies, (2) sharing personal information with third parties, and (3) the ineffectiveness of current privacy notices and license agreements because consumers do not read or understand them. Senator John Kerry announced that he planned to introduce legislation later this summer to meet the challenges new business models, social networking and new media, and behavioral advertising has presented to privacy. Of late, because of the confusion surrounding privacy, security, and cyber-security issues and the possible remedies to the problems emanating from exponential digital growth, the Congress has agreed to a hiatus in the debate and is hopeful that a legislative package from the Obama administration will be proposed to address these concerns.[9]

III. THE CONSULTATIONS OF THE EUROPEAN COMMISSION – REVIEW OF THE DATA PROTECTION DIRECTIVE (95/46/EC)[10]

On July 9, 2009, the European Commission initiated a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation, the Commission asked for advice on the challenges new technologies present to protecting personal data, in particular with the advances made in social media, behavioral advertising and the phenomenon of cloud computing. Central to its inquiry is whether the directive as currently constructed still meets the essential goal of protecting privacy as a fundamental right and, if not, what changes are needed in light of exponential technological advancement to reboot the directive's provisions.

The Article 29 Working Party on Data Protection, an advisory body on data protection and privacy, created by the Directive and composed of the national data protection authorities of the member states of the European Union in partnership with the Working Party on Police and Justice submitted their contributions to the Commission on December 1, 2009.[11]

Building on the foundational Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108)[12] and the Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8)[13] established the concept of privacy as a fundamental human right. The Treaty of Lisbon which entered into force on December 1, 2009, made the Charter of Fundamental Rights of the European Union binding on all member states plus introduced

9 See Consumer Online Privacy, U.S. Senate Committee on Commerce, Science, and Transportation, July 27, 2010, *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235#hearingParticipants.

10 Directive 95/46/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281, at 31.

11 *See* "The Future of Privacy," Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, *available at* http://ec.europa.eu/justice_home/fsj/privacy/index.htm.

12 ETS No. 108, 28.01.1981.

13 ETS No. 005, 11.4.1950

Article 16 of the Treaty on the Functioning of the European Union (TFEU) as a new legal basis for data protection applicable to the public and private sectors including the areas of law enforcement, judicial cooperation, and common foreign and security policy. The Treaty had the effect of dissolving the pillars that heretofore separated these components within the EU.[14]

The recommendations include the following:

- Clarify the application of some key rules and principles of data protection (such as consent and transparency);
- Innovate the framework by introducing additional principles (such as 'privacy by design' and 'accountability');
- Strengthen the effectiveness of the system by modernizing arrangements in Directive 95/46/EC (e.g., by limiting bureaucratic burdens); and
- Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

Chapter three of the recommendations, Globalization, notes that as a fundamental right, EU citizens should be guaranteed protection insofar as member states have jurisdiction but also infer that individuals can claim protection if their data is processed outside the EU. However, the scope of the directive's reach is not clear and lack of harmonization across member states causes confusion. For the private sector, legal certainty may mean one thing in Spain and another in the United Kingdom.

In general, most of the EU-based institutions, governmental bodies, and individuals support a strengthened legal framework with enhance obligations placed on the data controllers, ISPs, social network services, and cloud computing service providers.

The Information Commissioner's Office of the United Kingdom sponsored its own study, "A Review of the European Data Protection Directive" by Rand Europe in May 2009.[15] The report details the history, evolution, and present state of the directive, its enforcement, strengths and weaknesses. The authors' analysis is founded on this approach and balanced with the revolutionary technologies that have been deployed to the global community since the directive was implemented in 1998. Several of these recommendations include:

- Member States need to seek agreement on efficient interpretation, implementation and enforcement of the Directive (harmonization across MS boundaries) including encouragement of a risk-based approach; encourage Binding Corporate Rules (BCRs) may be more easily used to legitimatize cross border data transfers to third countries;
- The EC should improve the effectiveness of the Adequacy Rule and facilitate use of alternatives to this rule including BCRs and contractual clauses;

14 *See* "The Future of Privacy," *supra,* at 5.
15 *See* Review of the European Data Protection Directive, May 2009, *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.

- The Directive should specifically be included in the list of laws to be reviewed as part of the Better Regulation agenda;

- The principle, 'privacy by design' should be introduced in the new framework which should be binding for technology designers and producers as well as for data controllers who acquire and use ICT;

- Implement privacy enhancing technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data.

These concentrate on the role of the data controller and the manufacturer, designer, and procurer of ICT for processing, storing, or otherwise using personal data. The Rand study also discusses the role of the data subject – the EU citizen – as an ingredient in revising the directive and improving its utility as a tool to protect data in the region. The authors call for 'empowering the data subject' by recognizing that the behavior and role of the data subjects have changed since the directive's conception in the 1970's and enactment in 1995.[16] The report calls for the following enhancements to the new framework:

- Improving redress mechanisms that give the data subject more options to enforce his rights including court proceeding; consideration should be given to allow class action procedures under the directive;

- Compliant procedures should be refined, streamlined, and accessible as well as affordable and if these procedures do not yield results, alternative dispute resolution (ADR) ought to be provided by industry to remedy the complaint.

These latter recommendations strike a familiar tone with those in the United States who are accustomed to the use of independent third parties to mediate outstanding disputes which are often paid for by industry. Right of private action and class actions civil procedures are also tools available in the United States to seek redress of wrongs. Other themes that ring familiar are transparency (data breach notification when there is a likelihood of harm), notification of how data is being used in clear, unambiguous language, clarification on what informed consent in the Directive connotes and whether it is freely given.

At the American Chamber of Commerce to the European Union in Brussels on June 22, 2010, Viviane Reding, vice president of the European Commission for Justice, Fundamental Rights, and Citizenship, explained the transformational nature of the digital age and its consequences for meeting the challenges of protecting fundamental rights in the European Union. And although some within the data protection field characterize the advent of social network services, mobile technologies, cloud computing, and other technologies collectively as a digital tsunami, Ms. Reding's views these innovations as a means of improving the EU's economic performance and accelerating the use of electronic commerce to stimulate growth. In her speech to the chamber, she noted two challenges.

- "First, regulatory barriers are still holding back the potential for a real Single Market for e-commerce. We need to boost consumers' and businesses' confidence in a truly pan-European online marketplace; and

16 *Id.* at 15.

- Second, we need to modernize our data protection rules, which date from 1995. We need to build up a trusted environment for the use of personal data."[17]

Her remarks covered a range of both e-commerce, data protection, and privacy issues that recognized the potential for €3 billion in online behavioral advertising income in 2012 alone which represents an eight-fold increase over 2007. Still, data protection and privacy loom as major disincentives to online growth and deployment of new technologies and services. The consultations under way and the directive's review aim to strengthen enforcement while recognizing that consumers have both responsibilities and concerns over how their online activities and data are collected, tracked, and used. A prevailing theme in the comments submitted during the consultation was "a right to be forgotten." This idea has gained prominence among many of the leading thinkers in civil society and academia (see the Trends section). Ultimately, her overarching objective is to achieve clarity that protects the interests and fundamental rights of the data subjects while advancing technology to meet the challenges and opportunities of the digital age.[18]

Harmonization is critical to implementing the Directive and as Ms. Reding noted in her address to the Article 29 Working Party on July 14, 2010, her principal objectives in moving forward are based on the need for a 'comprehensive and coherent approach' that assures personal data protection and privacy are respected within the EU. Her chief themes for achieving this end are:

- Strengthen individuals' rights by ensuring they enjoy a high level of protection….particularly important in the online environment; transparency, and clear information from data controllers on how their information may be collected and processed;

- The internal market requires that personal data may flow across member states' borders freely and safely so their fundamental rights are protected. Thus, they need to know what their rights are and how to exercise them without undue constraints and these characteristics must be across member states' boundaries and insure that a level playing field is established. Currently, there is a clear lack of legal certainty and harmonization in implementing the Directive;

- The current rules on data protection in the area of police cooperation in criminal matters need revision;

- Data must be adequately protected when transferred outside the EU; current procedures for such transfers must be strengthened at the international level; and

- Implementation and enforcement of the existing rules are essential and the role of the Data Protection Authorities in the Member States should be strengthened to achieve consistent enforcement of the Directive's provisions.[19]

While several of Commissioner Reding's themes correspond to those outlined in the ICO's study, there is less emphasis on empowering the data subject and using dispute

17 Viviane Reding, "Building Trust in Europe's Online Single Market," Speech before the American Chamber of Commerce to the European Union, Brussels, Belgium (June 22, 2010).
18 *Id.*
19 Viviane Reding, "Towards a true Single Market of data protection," Speech before the Article 29 Working Party on Data Protection, Brussels, Belgium (July 14, 2010).

resolution bodies, and trustmark entities to build trust among EU citizens which would help advance the use of electronic commerce in the community and stimulate economic growth. As the debate continues within EU institutions, the options for revising the Directive will no doubt evolve and re-examine the important role the data subjects have in the legal framework.

A consensus seems to be emerging within EU bodies that identify common threads which should be incorporated into any revision of the legal framework for data protection. Peter Hustinx, the European Data Protection Supervisor (EDPS), noted in his address at the 23rd Annual International Conference, Cambridge, England, on July 6, 2010, that the current landscape is a complex one. The "Data Deluge" offers tremendous potential but also increasing threats to personal freedom and privacy.[20] Punctuating his presentation were the central themes of adaptation to the digital age, the role of the Commission and data protection authorities, use of new tools such as 'privacy by design' and privacy enhancement technologies, and empowerment of data subjects to exercise their rights to redress wrongs in the online world. Mr. Hustinx stressed the importance of effective protection and harmonization across member states' boundaries. Finally, he closed observing – perhaps in an understatement – that privacy is a hot issue, relevant to building trust and security, and must be built in from the start. How it is done is the challenge.

So we see emerging a body of ideas that suggest enhanced authority for data protection authorities, technology neutrality may be weakened for certain key sectors such as health care and finance, legal rights of redress for citizens including class actions, transparency and clarity for the consumer, and trust and confidence overall for both consumers and business. How exactly this will be molded into a new framework remains to be seen and Mr. Hustinx's view was that it would be at least two to three years before and any changes are realized. Any changes would nonetheless need to be approved by the European Parliament whose views remain opaque in the debate.

IV. BITS, BYTES, AND TRENDS IN THE FUTURE OF PRIVACY…IS THERE ONE?

To grapple with the complex issue of how to protect a person's identity, data, and personal reputation in a more effective and responsible manner than what is currently practiced – both in the United States and abroad – some of the more creative thinkers in the privacy arena have promulgated a number of paradigms that are worthy of consideration. Cloud computing's emergence and adoption has prompted many governmental institutions, civil society organizations, and academia to challenge the prevailing models based on civil or common law and the fair information practice principles (FIPPs) as meaningful solutions when data traverses the world instantaneously and is accessible by virtually anyone. Data breaches expose millions to potential harm and notification laws, particularly in the United States, have imposed obligations on the private sector to craft new business practices to comply. One of the first proposals for improving effective data protection is 'Privacy by Design'.

First attributed to the province of Ontario's information and privacy commissioner, Ann Cavoukian, privacy by design (P_bD) "refers to the philosophy and approach of embedding privacy into the design specifications of various technologies….achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and

20 *The Data Deluge,* THE ECONOMIST, Feb. 25, 2010.

processes."[21] Conceived by Doctor Cavoukian in the 1990s, P_bD has seven foundational principles that broad concept that digresses from the regulatory approach which held currency in the late 1990s and into the 21st century as the sole instrumentality for enforcing citizen and consumer rights. The principles are:

- Recognition that privacy interests and concerns must be addressed ***proactively***;
- Application of core principles expressing universal spheres of privacy protection;
- Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle – end to end;
- Need for qualified privacy leadership and/or professional input;
- Adoption and integration of privacy-enhancing technologies (PETs);
- Embedding privacy as a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality; and
- Respect for users' privacy.[22]

The P_bD approach offers positive benefits to businesses that adopt and implement these principles consonant with sound business practices that manage information wisely. By actively developing business practices that safeguard clients' personal data, organizations, as Christopher Graham, the Information Commissioner of the United Kingdom's Information Commissioner Office (ICO) build not only trust with their constituencies but they also build reputation online thereby creating an intangible asset that has value and which may be used to expand one's business.

Since its conception, the model has gained wide acceptance within the business community and civil society. Moreover, the European Commission has embraced the concept philosophically and has repeatedly cited the need for businesses to employ 'privacy by design' when producing new technologies, operating systems, or managing databases. These are further extended to encompass business practices, infrastructure, and physical design processes.[23]

While not widely adopted, it is believed that enforcement authorities' continued advocacy, especially in Europe, will lead to a comprehensive change in how enterprises think about privacy in their business plans. This development reminds one of the tasks chief privacy officers have in convincing executive management and business unit heads to think differently when managing personal data and compliance. Data is now a strategic asset to be managed and protected as much as an organization's intellectual property. Do it properly and the investment will pay off. To obtain management buy-in has been perhaps the most significant hindrance to introducing privacy by design systematically.

21 Ann Cavoukian, Ph.D., "Privacy by Design," Jan. 27, 2009, *available at* http://www.privacybydesign.ca/about/principles/.
22 *Id.*
23 *Id.*

Another concept that has gained recognition of late is Accountability and Harm. Accountability is one of the foundational principles of the Asia Pacific Economic Cooperation's (APEC) Privacy Framework which is nearing implementation. The Accountability principle rather being a standalone model is integrated with other principles based on the Organization for Economic Cooperation and Development's (OECD) privacy guidelines. The accountability principle states "A data controller should be accountable for complying with measures which give effect to the [material] principles stated above". Noting the importance of holding data controllers accountable for misusing personal data, the International Conference of Data Protection and Privacy Commissioners in deliberations to draft what became known as the Madrid Resolution that proposed new international privacy standards wrote the concept into the principles.[24] Work conducted under the aegis of the Joint Technical Committee 1 of the International Standards Organization also introduced accountability to the draft ISO privacy framework standard, 29100 which is expected to be adopted and reported in autumn 2010.

In the United States, accountability and harm are concepts that determine in some instances whether, for example, to issue notices to individuals when a data breach occurs. If the likelihood of exposed personal data will result in measurable harm to the person, then notice may not be required under various data breach notification laws. Conversely, if harm is likely to occur, then notification is required and costs incurred for complying are substantial especially when hundreds of thousands of records are involved. How to assess harm and to what degree are sanctions applied is the province of proportionality. Harm-based sanctions are applied in accordance with the degree of injury in a misuse of personal data, whether stemming from a data breach, use by the data holder for a purpose other than it was collected, or transfer to a third party for processing without the user's knowledge or approval.

Underpinning the APEC Privacy Framework is the use of "accountability agents" whose responsibility is to conduct organizational assessments of applicants who seek "certification" under the Framework's cross border privacy rule" and who may be found in default of complying with their own commitments following independent review. Although loosely analogous to the dispute resolution feature in the U.S.-EU Safe Harbor Framework, accountability agents have greater obligations because of their roles as certifying bodies within the Framework unlike is Safe Harbor where the U.S. Department of Commerce serves as the authority for reviewing applications submitted by the private sector.

The upcoming 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem has the theme "Privacy: Generations" inferring perhaps there is a generational divide on the concept of privacy and the "right to be alone." Indeed, Yoram Hacohen, the head of the Israeli Law, Information and Technology Authority notes on the conference's website:

> "Today, privacy stands at a crossroads. The existing legal and regulatory frameworks, in the EU, US, and OECD, as well as in Israel, date back to the 1980s and 1990s. They predate a new generation of technologies – including mobile devices, biometrics, RFID, cloud computing, indeed, the Internet itself – which has swept through the marketplace with such force so as to destabilize laws and regulations. They have seen shifts in the perception of privacy among a new

24 The responsible person shall: "a. Take all the necessary measures to observe the principles and obligations set out in this document and in the applicable national legislation, and b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23."

> generation of users, who post personal information and communicate with friends and colleagues on social networks. Policymakers all over the world realize that this sea change calls for a new generation of governance."[25]

Still, the debate over which legal framework ought to serve as the model for protecting privacy and data on a global basis remains a hot topic and calls for a United Nations convention on privacy may find their way into the conference's resolution. Another question that has been raised for a number of years is – does privacy really matter in the digital age where data is omnipresent and universally accessed? Technology adopters post their most intimate personal details on social networks and share information freely seemingly oblivious to the consequences later in life.

Jeffry Rosen, a law professor at the George Washington University and perhaps one of the seminal thinkers on privacy wrote in *The New York Times Magazine* about how "The Web Means the End of Forgetting."[26] His piece is a panoply on "the perils of the digital age" wherein companies routinely canvas social network sites seeking information – usually derogatory – on prospective employees (Microsoft reports that 75 percent of U.S. recruiters and human resources professionals are required to do online research about candidates).[27] A similar percentage report that they rejected applicants because of what they found online. Professor Rosen wrote that Facebook's 500 million users who represent 22 percent of all Internet users, post a phenomenal 55 billion pieces of content each month and that on average each member posts 70 pieces per month. How does one design a privacy framework capable of providing effective protection without taking into account the role of the user in exercising prudent judgment when sharing information?

In further citations, the article discusses how bad information about people has a much longer shelf life, attracts more viewers (voyeurs?), and remains in memory whereas good deeds are forgotten. In particular, he quotes the author of "Delete: The Virtue of Forgetting in the Digital Age," by the scholar Viktor Mayer-Schönberger. "By 'erasing external memories,' our society accepts that human beings evolve over time, that we have the capacity to learn from past experiences and adjust our behavior." However, in a society where everything is recorded, Schönberger writes that the things we did in the past are forever with us throughout our lives. The ultimate lesson, he says is that "without some form of forgetting, forgiving becomes a difficult undertaking."

So, one asks is privacy really drifting into oblivion and is it impossible to protect either as a fundamental right or consumer's right? Everyone it seems is searching for answers and no one proposal has universal appeal. Alex Turk, the French data protection commissioner has called for "a constitutional right to oblivion" that would allow citizens to maintain a greater degree of anonymity online and in public places.[28] But reputations are destroyed and businesses flourish to correct online errors and restore one's public persona. Should people have a public and private self and should bad reputations have a sunset provision as Jonathan Zittrain, Harvard Law School professor recommends?[29] These ideas are worthy of consideration, debate, and perhaps implementation. But how?

Today, everyone may have their fifteen minutes or seconds of fame and have a global audience witness their moment in time. The perceived generational divide between

25 See http://www.privacyconference2010.org/ for details on the conference's agenda, speakers, and events.
26 Jeffrey Rosen, *The Web Means the End of Forgetting*, THE NEW YORK TIMES MAGAZINE, July 21, 2010.
27 Ibid.
28 *Id.*
29 *Id.*

the young and old is due to technology's reach and ease of use with high school and college students who thrive online and their parents whose remembrance of things past fades as time marches on. For those on the Internet, the past is preserved forever and the question of "how much privacy people can expect – or even desire – in the age of ubiquitous networking" looms large.[30]

For professor Solove, the future of reputation is also a concern as "broad-based exposure of personal information diminishes the ability to protect reputation by shaping the image that is presented to others."[31] It was thought early in its developmental stages and later in the early days of diffusion, the Internet would be a highway for global data sharing of ideas, economic stimulation, improved healthcare and education, enhanced government-centric online services, and for some the liberation from intolerance. However, backlashes from countries such as China, Burma, some of the Arabian gulf states and others who impose limits on Google, RIM (BlackBerry), and others may have the opposite effect with historical antecedents – the cyber list makers. In the words of professor Solove, "what is to be done?" As before, personal control over how one's personal information is used is central to the new privacy world. Professor Solove, recognizing that privacy laws in the United States are less stringent than in other jurisdictions suggests new legal measures, e.g., the U.S. should recognize that a person doesn't sacrifice all privacy rights when appearing in public.[32]

Recently, *The Wall Street Journal* published a three-part series on how companies use the Web to mine data and generally spy on consumers' web-based practices, preferences, and tastes. The *Journal's* first article highlighted companies that use aggregated personal information ostensibly de-identified to package and market profiles to their clients. By employing web beacons, cookies, and other technological-based web tools to track consumers' activities online.[33]

Considering the ongoing debate about privacy and data protection, it is instructive to understand how personal data of citizens/consumers is collected, packaged, and "sold on stock-market-like exchanges that have sprung up in the last 18 months."[34] One of the most revealing findings of the study conducted by the WSJ was that the top 50 websites in the country installed, on average, "64 pieces of tracking technology on the computers of visitors, usually with no warning. A dozen sites installed more than a hundred; Wikipedia installed none.[35]

Many service providers track our tastes and preferences to better serve us and to offer content that meets our interests. That these interests are recorded without our knowledge has had little impact on our – aggregate sense – outrage or sense of violation suggests our level of indignity or concern that our privacy has been violated is negligible. We may find that such services are benign and pose no material threat to our identity or security. Still, those same technologies that track our web presence may also be used for nefarious purposes including identity theft for purposes of committing fraud.

Paul Ohm, an associate professor at the University of Colorado law school, notes that there is ample data around to uniquely identify individuals and that information-science researchers are able to piece together seemingly unrelated "bits" to re-identify

30 Daniel J. Solove, *The End of Privacy?,* SCIENTIFIC AMERICAN, Sept. 2008, at 101.
31 *Id.* at 103.
32 *Id.* at 104.
33 Julia Angwin, *The Web's New Gold Mine: Your Secrets,* THE WALL STREET JOURNAL, July 30, 2010.
34 *Id.*
35 *Id.*

people. In fact, these researchers have calculated that only 33 bits are required (one bit being equivalent to two values 0 and 1 or on and off.[36]

With the world awash with an ocean of data and technological tools increasingly adept at gleaning the minutest bit of information from online users' pursuits, how is it possible to guarantee one's privacy and anonymity in the digital age? Is it an aspiration that is unachievable and whose data is it anyway?

We've seen glimpses of models that are harm-based, that discuss accountability and writings that demand that privacy be baked into design, technology development, and business practices. Still, the question of whose data is it only has been resolved in the European Union's data protection directive and in the charter of the European Union where data protection is a fundamental human right. By 2011, it is estimated that more than 1,750 exabytes of data will be created outpacing the production of available data storage by nearly 1,000 exabytes.[37]

The Economist's special report on managing information noted that Wal-Mart "handles more than 1 million customer transactions every hour, feeding databases estimated at more than 2.5 petabytes—the equivalent of 167 times the books in the Library of Congress…Facebook is home to more than 40 billion photos."[38]

IV. CONCLUSION

Just how government and industry and in a larger sense, society, addresses these issues will determine whether as Justice Brandeis wrote, privacy is the right to be left alone. Is it possible in the world we live in today? Are there models yet to be discovered that will assure privacy and are we truly alone now? Will Privacy 3.0 be compatible with Web 3.0 and when we refer to the ocean of data that immerses the digital world, is there one global model that meets the needs of different cultures, customs, and political structures that all may agree serves disparate purposes? In the film, Dr. Zhivago, Strelnikov, a notoriously brutal Red Army commander, meets Yuri on a railroad siding in Siberia. When Yuri mentions Lara, Strelnikov observes:

"*The personal life is dead in Russia. History has killed it….the private life is dead.*"

Is privacy an ideal that will never be attained? Has technology killed it?

36 Julia Angwin & Jennifer Valention-DeVries, *The Information That is Needed to Identify You: 33 Bits,* THE WALL STREET JOURNAL BLOG, Aug. 4, 2010.
37 *Data, data everywhere,* THE ECONOMIST, Feb. 25, 2010.
38 *Id.*