.Net Passport Under The Scrutiny Of U.S. And EU Privacy Law: Implications For The Future Of Online Authentication

OLENA DMYTRENKO & ALI NARDALI*

ABSTRACT

The new era of Internet-based, multi-national communication has produced myriad of difficulties, difficulties the law has never encountered before. The difficulties are unique, we feel, because they often juxtapose popular ancient concepts with new and novel problems. One such difficulty has to do with the juxtaposition of the age-old concept of individual privacy with Internet security. This is the difficult we explore in this Article. Specifically, we sketch the developing tension between protecting online privacy and universal online authentication vis-à-vis Microsoft Corporation's .Net Password architecture. Furthermore, we highlight areas of research, along the way, that we feel are amenable to further scholarship.

I. THE RECENT CONTROVERSY OVER MICROSOFT-BASED .NET PASSPORT'S IMPOSITION UPON ONLINE CONSUMER PRIVACY

1. REAL NEEDS AND REAL PROBLEMS: THE CREATION OF .NET PASSPORT

The decentralized character of the Internet allows users to post and collect information anonymously. As a result, the Internet opens unique opportunities for the promotion of free speech and expression—that is, the anonymous nature of the Internet allows individuals and collective entities to convey and express ideas that in non-anonymous circumstances would perhaps go unuttered. But the Internet also creates significant challenges. Take, for example, the

---

* Olena Dmytrenko - LL.M, University of Washington School of Law. Ali Nardali - J.D. Candidate, Yale Law School.

Ms. Dmytrenko thanks Professor Jane Winn of the University of Washington School of Law for her gracious guidance and advice in the preparation of this article, and Cedric Laurant of the Electronic Privacy Information Center for his comments, critiques and encouragements.

fast-growing number of businesses that choose to provide goods and services on the worldwide network. From a security perspective, how will these businesses ("sites") determine whether an online customer ("client") is trustworthy and qualified enough to perform a contract-based transaction with the site? Before shipment, how will a Stradivarius supplier in Vienna trust that an order for one of his rare violins is not from some ten-year-old Californian gone wild with a stolen credit card? With an eye towards marketing, in what way can these sites learn more about their unseen clients—about their tastes and preferences—to provide more attractive goods and services? In the run-of-the-mill market, merchants see and talk to their clients, noting subtleties in behavior and implementing marketing strategies accordingly. Can something analogous to this be achieved on the Internet?

With these questions in mind, sites are increasingly requiring clients to provide personal information to facilitate enhanced security and marketing efficacy. A client's birthday, for example, could function as a data point with which sites can crosscheck and corroborate credit card orders. The birthday datum could further serve as a marketing device, generating effective, age-specific marketing techniques. In addition to security- and marketing-based concerns, sites that are interested in creating fast and efficient payment methods—by drawing clients and online payment devices closer together—are beginning to require that clients provide personal information. For example, a site may require that first-time clients provide both their name and birthday in addition to their credit card information. Such a scheme would permit returning clients to execute transactions using their name and birthday only—the sixteen-digit credit card numeric would no longer be necessary. Hence, client-specific personal information promotes faster, less-exhausting, and more client-friendly transactions.

According to the Internet Law and Policy Forum, "authentication means confirming the identity of a [client]. [Sites]...desire authentication of [clients]...[to] promote[ ] [site] comfort that the transaction is legitimately placed and provides potential recourse in the event there is a problem."[1] Authentication is associated with, and often mistaken for, "identification."[2] Identification is defined as

---

[1] Internet Law and Policy Forum, *The Role of Certification Authorities in Consumer Transactions*, *at* http://www.ilpf.org/groups/ca/back.htm (last visited Dec. 14, 2004).

[2] AMETAS, *Users Guide:A-H*, *at* http://www.accsis.com/ametas/docs/UsersGuide/gl01.html (last visited Dec. 14, 2004).

"using claimed or observed attributes of an individual to infer who the individual is."[3] Authentication is a process by which clients receive authorization to perform some online transaction—for example, to purchase good A.[4] Identification is a process by which clients provide some personal trait with which a site may be able to recognize them in the future—for example, a client's birthday.[5] Authentication does not require identification—clients do not have to provide personal information in order to gain authorization for a transaction, much as run-of-the-mill customers do not have to provide personal information to purchase a good at a grocery store.[6]

Sites often require new clients to create a username and a corresponding password. Many require that clients provide identification, such as name, address, birth date, and so on. Some gather further information, called profile information, through which they ascertain client occupations, hobbies, travel preferences, and the like. Profile information allows a site to improve its marketing regime and to provide clients with preferred products, the revenues of which subsidize the site's operation costs.

Authentication systems, even the simplest ones, pose formidable challenges to both sites and clients. Entering and re-entering variant information, such as variant usernames and passwords, for different sites irritates and interrupts the search process.[7] In January 2002, Jupiter Media Metrix found that the use of variant usernames and passwords bothered forty-two percent of online customers and that almost twenty-nine percent of them believed that the customer service could be improved by developing a simpler web-site sign in process.[8] Entering and re-entering variant information gives rise to another challenge in authentication systems—Internet users lose or forget

---

[3] Authentication Privacy Principles Working Group, *Interim Report: Privacy Principles for Authentication Systems*, *at* http://www.cdt.org/privacy/authentication/030513interim.pdf (last visited Oct. 29, 2003).

[4] Internet Law and Policy Forum, *supra* note 1.

[5] Authentication Privacy Principles Working Group, *supra* note 3.

[6] AMETAS, *supra* note 2.

[7] *Id.*

[8] Microsoft.net Passport, *Review Guide*, at 3, *at* http://download.microsoft.com/download/a/f/4/af49b391-086e-4aa2-a84b-ef6d916b2f08/passport_reviewguide.doc (last visited Mar. 15, 2005) quoting Jupiter Media Metrix, *Helping Consumers Understand Security Risks of Online Registration and Storing Personal Information.* Primary Analyst: Rob Leathern.

passwords, given their number and variation.[9] This, along with the fear of losing future passwords, creates a significant barrier to usage, resulting in the under-utilization of pre-existing Internet and site infrastructure. Lost passwords also increase the cost of customer service.[10] Last but not least, the irritation and fear caused by the use of variant passwords pressure Internet users to use identical usernames and passwords across different sites, increasing the risk of online identity theft.

Influenced by these difficulties, Microsoft Corporation ("Microsoft") revolutionized the Internet by developing a universal sign-in mechanism for multi-site surfing in 1999. The cutting-edge program, first known as Microsoft Passport and later renamed .NET Passport, resolved the difficulties in two ways. First, it allowed clients to enjoy one sign-in portal, with one username and one password, from which they could access multiple participating sites. Second, it eliminated the need for individual sites to authenticate or identify clients, reducing operation costs for participating sites—thus, a participating site would not have to determine whether a client met the requirements for buying good A.[11]

The .NET Passport ("Passport") architecture is based on a single authentication server operated by Microsoft. Passport clients are assigned unique usernames, called Passport Unique Identifications (PUIDs), with which they log on to the Passport server.[12]

Passport was initially designed to collect a vast array of information from clients, which could be split up into three conventional blocks. The first contained minimal information: a client's username (i.e., a functional e-mail account) and password, both necessary to log in. The second block, named credentials, contained information that enabled clients to retrieve lost or forgotten passwords. For example, in the event of a lost or forgotten password, Passport prompted a client-chosen secret question. If the client answered the question correctly, Passport supplied the forgotten password. The third block, named maximal profile information,

---

[9] Trustgenix, *Free Whitepaper: Enabling Single Sign-On Through Identity Federation, Executive Summary, at* http://www.trustgenix.com/whitepaper (last visited Oct. 30, 2003).

[10] *Id.*

[11] Microsoft.net Passport, *Review Guide,* at 3, *at* http://download.microsoft.com/download/a/f/4/af49b391-086e-4aa2-a84b-ef6d916b2f08/passport_reviewguide.doc (last visited Mar. 15, 2005).

[12] *Id.* at 10.

contained personal information about clients, such as gender, birthdate, occupation and the time zone in which the client was located. This last block was also capable of containing pictures of clients and their loved ones.[13]

To promote Passport, Microsoft made access to many of its popular online services—such as online instant messaging, Hotmail, and online assistance for Microsoft products—contingent on the creation of an individual Passport account. In accordance to Microsoft, by 2003, Passport had over 200 million subscribers worldwide,[14] performing an astounding 3.5 billion authentications per month.[15] It included about eighty participating sites.[16] All was going well for Passport and Microsoft, until a colossal turmoil of criticism dawned on the horizon.

2. THE VALUE OF PERSONAL INFORMATION IN BUSINESS TRANSACTIONS ON THE INTERNET

For a variety of reasons, cultures that embrace the Internet have become increasingly conscious of volunteering personal information on the Internet. The most immediate reason is protection. Like most human beings, individual clients derive psychological satisfaction from knowing that their personal information is protected. An individual's ability to find a good job, secure an affordable mortgage rate, and obtain preferred healthcare depends on the information available about that individual in society. When every transaction that a consumer makes is being compiled, manipulated, analyzed, and reanalyzed, the chances for mistakes increase. Even if all of the data collected appears to be accurate, is there a social value in encouraging creation of comprehensive internet data warehouses managed by private businesses? As Challis and Cavoucian suggest:

---

[13] In the Matter of Microsoft Corp., Complaint and Request for Injunction, Request for Investigation and for Other Relief, at 7, *at* http://www.epic.org/privacy/consumer/MS_complaint.pdf (last visited Nov. 1, 2004) [hereinafter Complaint].

[14] Joe Wilcox, *Study: Customers Wary of Online IDs,* CNET NEWS.COM, ¶21 *(*Apr. 26, 2002*) at* http://news.com.com/2100-1001_3-892808.html (last visited Nov. 21 2004).

[15] Microsoft.net Passport, *supra* note 11, at 3; World LII, EPIC Alert (Jan. 31, 2003), *at* http://www.worldlii.org/int/journals/EPICAlert/2003/2.html (last visited Apr. 5, 2005).

[16] Seppo Heikkinen, *Identity Management*, at 92, *at* http://www.cs.uta.fi/reports/bsarja/B-2004-8.pdf (last visited Apr. 5, 2005).

> If the totality of every person's online experience is captured, warehoused, profiled and data-mined, human behavior can be adversely and ineluctably altered on an individual and societal basis....Individuals are manipulated according to a set of rules or code that lurks somewhere behind their computer screens, and of which they are only vaguely aware.[17]

Jupiter Media Metrix found that the protection of personal information on the Internet could cost sites $25 billion by 2006,[18] absorbing capital that could otherwise be spent in more efficient ways. Further, a U.S. Federal State Commission report, released in 2000, found that ninety-two percent of clients were concerned (and sixty-seven percent very concerned) about the level of protection, deterring commercial activity from otherwise taking place. In fact, consumers who had never made an online purchase identified protection as a key reason for their inaction.[19] Avivah Litan, a leading Gartner analyst, has concluded: "[p]eople are paranoid; they don't want to give their information away and they have a right to be paranoid."[20] Ensuring protection, therefore, would substantially amplify the quantum of business activity on the Internet. But this approach is predicated on an important assumption—namely, that personal information is indispensable to Internet-based business transactions. Because Internet-based business transactions require personal information, and because potential clients tend to bear protection concerns that deter their participation in these transactions, then ensuring and providing superior protection mechanisms would, according to this line of thinking, enhance business.[21] If, however, personal information were not a requirement for participation in Internet-based transactions, then

---

[17] William S. Challis & Dr. Ann Cavoukian, *The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective,* 19 J. MARSHALL J. COMPUTER & INFO. L. 1, *35 (2000).

[18] Jupiter Media Metrix, Online Privacy Vision Report, at http://www.jup.com/bin/item.pl/search/ (last visited Oct. 30, 2003).

[19] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace,* at 2, (May 2000), *at* http://www.ftc.gov/reports/ privacy2000/privacy2000.pdf (last visited Nov. 1, 2003).

[20] Wilcox, supra note 14.

[21] *Id.*

potential clients would not harbor prohibitive protection concerns in the first place. Enhancing protection, therefore, appears to be just one way to boost business. Designing a platform through which Internet-based transactions can take place absent the need for clients' personal information is another viable route to achieving that end—a route that seems to be more consonant with Western notions of individual autonomy.

This begs the question: if online personal information management is accurate and protected, what social value exists in maintaining data warehouses managed by sites? Does the procurement of personal information from clients serve any social value aside from promoting efficient business on the Internet? And must personal data be obtained for efficient business on the Internet in the first place?

If anything, the social consequences of maintaining online personal information are damaging.[22] The bulk of scholarship that deals with the acquisition of online personal information centers on alleged violation of individual rights, individual autonomy, and individual dignity. A potentially fertile avenue of future scholarship is to examine the extent to which routine collection of personal information from individuals on the Internet affects aggregate social behavior *off* the Internet. If the personal information necessary to participate in ordinary transactions is volunteered by a subset of the population time and again, and if the cardinality of that subset is increasing more and more as members of society begin to participate in Internet-based transactions, would the importance that a society places on the privacy of personal information *off* the Internet eventually diminish? Could repeated production of individual personal information on the Internet eventually transform individual and mass-aggregate mentalities so that, for example, there would come a day when no American would be upset by having to produce her birth date to obtain a gallon of milk? The point should be clear: the procurement of personal information on the Internet lacks any social value outside of promoting efficient business and, in point of fact, may encourage a diminution in the premium society places on the privacy of personal information *off* the Internet.

---

[22] *See* Challis & Cavoukian, *supra* note 17, at *35.

3. DIFFERING STANDARDS OF PROTECTION BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

In an effort to protect the interests of both clients and sites, governments around the world have developed varying policies addressing the protection of personal information online ("protection").[23]

Some claim that the European Union ("EU") is the trendsetter in addressing protection.[24] Under the EU 95/46/EC Data Protection Directive, all Member States must "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[25] Under the Directive, personal information data ("data") may be collected, stored, retrieved, or processed under limited circumstances: (a) clients must unambiguously consent to data collection; (b) the purpose for the procurement of data must be legitimate; (c) clients must know site identity and site interest in the data; (d) clients must have ready access to data that pertains to them; (e) clients must have the ability to object to the use of any data that pertains to them; and (f) data must not be the sole basis on which important decisions—including work ability, creditworthiness, and reliability—are based.[26] To ensure the implementation of these principles, the Directive further established the Working Party, an independent European advisory body on data protection.

In contrast to the EU, the United States has not passed any overarching legislation dealing with data protection. Several reasons may account for this. The U.S. adopted its Constitution centuries before protection became a concern among industrialized countries. Given the extensive and time-consuming process by which laws are made in the U.S., legislation that may significantly affect protection is

---

[23] *See, e.g.*, Council Directive 95/46/EC, 1995 O.J. (L281) 31 [hereinafter Directive]; Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391 (2002).

[24] Angela Vitale, *The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT'L L. 321, 322 (2002).

[25] Directive, *supra* note 23, art. 1.

[26] Huie, *supra* note 23, at 445.

likely to take longer to sanction and implement. In addition, as Joel Reidenberg observes, the European vision of governance "generally regards the state as the necessary player to frame the social community in which individuals develop and in which information practices must serve individual identity...Indeed, citizens trust government more than the private sector with personal information....Law enshrines prophylactic protection through comprehensive rights and responsibilities."[27]

Enacted laws in both the EU and the U.S. also afford some guidance in resolving the divergence in scope of legislation between the two entities. The EU regime stipulates that clients must unambiguously consent to the collection of personal data.[28] Under this regime, clients opt into a scheme in which they volunteer their personal information. They hold the freedom to choose whether they participate in a regime—a regime in which protection is a difficult issue. By contrast, the U.S. applies an opt out approach, which allows for the collection of data only if subjects have the option to terminate the process at will.[29] "U.S. privacy laws generally keep intact the rights of businesses to use personal data for marketing purposes, so long as they provide the consumer a choice to 'opt out' of participation—usually by checking a box on the company's Web site."[30] Whereas the EU legal scheme allows data collection only if clients initially consent, the U.S. scheme allows it only if the clients have the ability to opt out. This difference reflects a divergence of values between personal data protection and commercial data protection in the two cultures.[31] Kramer explains the divergence as follows: while Europeans treat privacy as a fundamental human right, Americans view it as a commodity that should be controlled through the free market. In the European mindset, personal information is closely connected with individual integrity and autonomy, so much so that to give it away is akin to giving up one's bodily organs. In the

---

[27] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 730-31 (2001).

[28] Directive, *supra* note 23, art. 1.

[29] Seagrumn Smith, *Microsoft and the European Union Face Off Over Internet Privacy Concerns*, 2002 DUKE L. & TECH. REV. 14.

[30] Jon Swartz & Byron Acohido, *EU Scrutinizes Microsoft's Passport*, USA TODAY, June 12, 2002, at 3B.

[31] *See generally* Lynn Chuang Kramer, *Private Eyes Are Watching You: Consumer Online Privacy Protection—Lessons from Home and Abroad*, 37 TEX. INT'L L.J. 387 (2002).

commodity-driven mindset of Americans, personal information is yet another good in the free marketplace, a good that an individual may elect to barter away.[32]

Thus, instead of an overarching regime as in Europe, the U.S. has adopted a series of discrete mechanisms designed to protect data that fall within some narrowly-drawn category of sensitive data—for example, medical (HIPAA), financial (Gramm-Leach-Bliley Act) and children's (COPPA) records that contain personal information. "Sectoral" categories such as these are afforded protection. Further, whereas the EU has created the Working Party, the U.S. has not created a special authoritative body on data protection. The U.S. Federal Trade Commission (FTC) acts on behalf of consumer protection complaints, but its "authority is restricted to a deceptive or unfair practice, which causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[33]

In spite of such sweeping differences between these two approaches, which give rise to heated debates among players from both sides of the Atlantic, the Passport case delivered a surprising result: both the EU and U.S. policies on protection supported and complemented one another. When brought together, the bi-partite legal scheme produced a sensible victory for privacy advocates worldwide.

4. WHY THE CLASH WITH PASSPORT?

Passport's implementation brought forth unprecedented turmoil among privacy advocates in Europe and the U.S. From the outset, Microsoft faced two distinct challenges: 1) the software behind Passport did not afford sufficient protection, and 2) Microsoft company policies allegedly disregarded consumer privacy and security.[34]

On the first count, Passport was scrutinized on three distinct grounds: (a) Passport could collect vast arrays of general profiling information with no legitimate reason in sight; (b) the designation of PUIDs to clients and the collection of data in a central repository provided Microsoft with the ability to process client information

---

[32] *Id.* at 390.

[33] Challis & Cavoukian, *supra* note 17, at *24.

[34] Complaint, *supra* note 13.

unilaterally without notice and consent; (c) Passport lacked adequate security standards, especially when it was employed from public computer portals.[35]

On the second count, Microsoft was scrutinized on three distinct grounds: (a) access to other Microsoft services, such as software support, was contingent upon Passport registration; (b) Microsoft ensured clients a high level of protection on its participating sites, when it merely required those sites to have a privacy policy and did not provide any baseline standards; (c) Microsoft possessed the ability to introduce fees for Passport services, such as access to clients' personal information, allowing financially-disadvantaged clients limited control over their own data.[36]

Convincing the EU and the U.S. to initiate an investigation based on these accusations was difficult, as neither had in place a mechanism for adjudication on the merits.

5. THE CONTROVERSY AND THE U.S.

The FTC, the sole agency capable of reviewing business-based protection complaints in the United States, does not assign a specific definition, value, or remedy to protection compromises *per se*; the FTC merely provides remedies against "unfair and deceptive trade practice[s]."[37] The analysis of the Federal Trade Commission Act[38] shows that, in fact, to obtain relief measures from the FTC, a complainant concerned of a privacy violation must show the following: (a) that a site imposed on client privacy; (b) that doing so caused (or could cause) a particular injury; (c) that the injury is (or could be) greater than the interest in a self-regulated and unrestricted market. If unmet, the FTC would side with the site; the American right to business self-regulation would triumph over the consumer right to protection of personal information.

Given this burden against the client, privacy advocates in the U.S.—the Electronic Privacy Information Center (EPIC) and twelve other leading consumer protection groups—filed a complaint with the FTC in July 2001, hoping for fragmentary relief at best; namely, to

---

[35] *Id.*

[36] *Id.*

[37] Federal Trade Commission Act, 15 U.S.C. § 45 (2005).

[38] *Id.*

enjoin Microsoft from alleged misrepresentations in marketing Passport to clients.[39] The privacy groups argued that profiling clients amounted to "unfair and deceptive practice"[40] and requested the FTC to enjoin Microsoft from violating §5 of the FTC Act, which refers to unfair and deceptive trade practices. In other words, the FTC did not predicate its case upon a violation of the privacy afforded to personal information—which some would consider a basic and fundamental human right. Because the FTC has jurisdiction in allegations of unfair and deceptive practice, this was the only viable way to initiate the battle.

6. THE CONTROVERSY AND THE EU

In contrast to the U.S., privacy complaints within the EU are adjudicated by determining whether the site violated a fundamental value in protection.[41] For sites that have been found to violate privacy regulations, the consequences can be heavy—when EU Commissioner Erik Meijer convinced EU authorities to investigate Passport allegations in May 2002, optimistic journalists reported: "[i]f Microsoft is found to have violated EU privacy rules, it could face fines and be ordered to squelch any offending activities. The EU also could order Passport pulled from the market."[42]

The legal issues involved in the EU investigation were much more complicated in structure than those portrayed by the media. Microsoft was not a EU-based company, and so its business practices could, at best, fall under the EU jurisdiction only as much as they affected the EU market. The worldwide availability of the Passport naturally triggered a question of the EU's ability to determine the Passport's fate for the EU consumers without affecting the interests of consumers outside the Union. Another difficulty was determining the authoritative entity that would handle the case: would it be a communal EU body or a member-state agency in charge of dealing with protection? A communal body—here, the Working Party—would lack any and all power of direct enforcement: as a European Commission spokesman once explained, "while the [collective]

---

[39] Complaint, *supra* note 13.

[40] Complaint, *supra* note 13.

[41] *See generally* Directive, *supra* note 23.

[42] Swartz & Acohido, supra note 30.

Commission has authority to help member states interpret European Community law, it lacks authority to investigate on its own."[43] The Data Protection Directive, which outlined the Working Party's primary legal framework, was intended to help member states implement nation-specific legislation; it was not designed as a statute that explicitly outlined sanctions for violations, let alone sanctions for violations by entities outside the EU's physical borders. The only courses of action available to the Working Party were written documents—a recommendation, an expert opinion, or, most potent, a report to the Commission that would invite it to take action if it thought action were necessary. That said, handing the matter to the Working Party would "produce one European answer," in both a cost and time-efficient manner.[44] Though a seemingly feeble declaration on its own, the Working Party statement would come from a unified and cohesive European body.

7. MICROSOFT'S REPLY TO BOTH THE EU AND THE U.S.

Microsoft initially denied all of the accusations outlined in the EPIC request to the FTC, declaring that EPIC's attack against Microsoft's efforts to provide consumers with a uniform method of doing business was intended to use "the trappings of a legal procedure to generate press attention for their own agendas and their own philosophical opposition to the technology itself, in whatever form it might be implemented."[45] Effectively using the limitations intrinsic to both the Working Party and the FTC, Microsoft dismembered privacy imposition into narrow and discrete structures, none of which could possibly be found illegal on its own. Microsoft argued to the FTC, for example, that the inability of clients to delete their Passport profiles complied with U.S. law: there was no law requiring that clients be able to delete their accounts.[46] Microsoft had never claimed, the company

---

[43] *EU Countries May Consider Microsoft Data Probe*, MERCURY NEWS.COM, May 27, 2002, *available at* http://www.siliconvalley.com/mld/siliconvalley/business/international/europe/3347830.htm?template=contentModules/printstory.jsp (last visited Mar. 17, 2005).

[44] *Id.*

[45] Microsoft, *Microsoft Privacy Priorities and Practices with Respect to the EPIC Complaint to the FTC: Facts and Clarifications, at* http://www.microsoft.com/presspass/features/2001/aug01/0824PrioritiesFS.asp (last visited Nov. 1, 2003).

[46] *Id.*

further argued, that clients could delete their Passport accounts.[47] Therefore, no "deception" existed. Microsoft additionally argued that the complainants failed to substantiate general allegations with specific examples: despite the subscription of millions of clients and the computation of billions of authentications on Passport, the complainants could not cite a single instance in which data was endangered.[48]

Microsoft initially reacted to EPIC's complaint aggressively stating that the complaint was "replete with factual errors, misrepresentations and speculations that demonstrate[d] fundamental misunderstandings of the products, services and technologies they challenge[d]" and was filed "solely on the basis that EPIC disagrees with or is dissatisfied with private-sector efforts to protect consumer privacy."[49] Nevertheless, the company eventually implemented changes to Passport that comported with EPIC's complaint and, thereby, gave a *prima facie* impression of deference to both the FTC and the Working Party.[50]

In spite of this appearance, there remains a question as to whether in fact deference and complaisance had anything to do with the matter. According to Adam Sohn, the Microsoft product manager for Passport implementation, the modifications that followed the Microsoft settlement with the FTC were already in the works: the modifications had very little, if anything, to do with the FTC complaint. "[The] process [of change] started a year ago...It's a regular update to the service....This is all stuff that's been in the works for some time."[51] Richard Smith, an independent security analyst, agrees: "Microsoft is just trying to clean up stuff...They're fixing some problems here in what is a natural evolution of Passport."[52]

---

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *See generally* In the Matter of Microsoft Corp., Agreement Containing Consent Order, File No. 012 2340, *at* http://www.ftc.gov/os/2002/08/microsoftagree.pdf (last visited Nov. 30, 2003) [hereinafter Agreement].

[51] *Microsoft Beefs Up Passport Security*, CNET News.com (Sept. 2, 2002), *at* http://ecoustics-cnet.com.com/Microsoft+beefs+up+Passport+security/2100-1001_3-956246.html (last visited Dec. 14, 2004).

[52] *Id.*

According to the above accounts, the modifications were already in the works; they would have been carried out with or without the EPIC-initiated complaint. If truthful, Sohn and Smith's comments prove a nasty setback for EPIC, the FTC, and the Working Party, who received much praise for their ostensible ability and power to effectuate such change. Evidence indicates, however, that Sohn and Smith provided at least a somewhat misleading account of the matter. If, as Microsoft strongly asserted at first, their behavior was not prohibited by the letter of the law, and if, as Sohn and Smith suggest, company modifications intended to repair objectionable—albeit legal—privacy matters were already in the works, why did the parties settle?

Brad Smith, Microsoft's general counsel, is on the record as stating that Microsoft believed that "...the agreement with the FTC would raise [the bar for Internet security and privacy] not only for Microsoft, but for the industry as a whole..."[53] "We realize – he continued, that some of our statements in the past could have been clearer and in some cases less enthusiastic. We've already changed them..."[54] This evidence suggests that Microsoft was in fact influenced by outside developments in a tangible way.

Even if Microsoft did not violate the law *de jure*, continued investigation into alleged violations of privacy rights would prove a public nightmare. The FTC's influence is supported by the fact that the settlement agreement stipulates that Microsoft will be levied $11,000 *per* violation *per* day for breaking any of its terms. Recall that by 2003 there were roughly 200 million subscribers on Passport. Using that figure, a Passport-wide security breach would cause Microsoft $2,750,000,000,000 *per* day—not a small order even for Microsoft. The quantum of power legal agencies yielded in transforming Microsoft's behavior remains a genuine question amenable to further scholarship.

The settlement agreements are outlined in four sets of documents: (a) the Agreement between Microsoft and the FTC; (b) an FTC Consent Order; (c) *Working Document on Online Authentication Systems* by the Working Party; and (d) Microsoft's new privacy policy on Passport utilization.

---

[53] Brad Smith, Q&A: Microsoft's Agreement with the Federal Trade Commission on Passport (Aug. 8, 2002) *at* http://www.microsoft.com/presspass/features/2002/aug02/08-08passport.asp (last visited May 16, 2005).

[54] *Id.*

8. MICROSOFT'S AGREEMENTS WITH THE U.S.

Under its settlement with the FTC, Microsoft agreed "not [to] misrepresent in any manner, expressly or by implication, its information practices" and to disclose sample reproductions of its marketing scheme to the FTC upon request.[55] It further promised to "establish and maintain a comprehensive information security program...designed to protect the security, confidentiality, and integrity of information collected from or about [clients]."[56] Backed by the Consent Order, the settlement stipulated that Microsoft undergo an independent audit and report any measures taken as a result to the FTC. Failure to follow the Consent Order would constitute a violation of the law and would entail civil penalties.[57]

9. MICROSOFT'S AGREEMENTS WITH THE EU

Due to the jurisdictional limitations, the Working Party in its capacity of an advisory body, could not afford an introduction of a strong enforcement mechanism or a penalty comparable to the FTC's $11,000 *per* day *per* violation.. On the other hand, it could afford, in contrast to the FTC, responding to a general privacy concern directly instead of tailoring the logic of the response to a concept of "deceptive trade practices." The analysis of the Working Document shows that the obligations it imposes on Microsoft form three logical clusters: (1) to provide users with more control regarding their own data; (2) to streamline communication to users regarding their privacy protection; and (3). to take efforts towards developing a more privacy-friendly technical architecture for the Passport.

To provide clients with more control over their data, the Working Document suggested the following: that clients have the capability to create pseudonymous accounts; that clients have the ability to delete Passport accounts with ease; that clients have the ability to omit data from their Passport profiles; and that clients have the ability to revise personal data with ease.[58]

---

[55] Agreement, *supra* note 50, at 3.

[56] *Id.* at 4.

[57] *Id.* at *2.*

[58] Article 29 Data Protection Working Party, *Working Document on On-line Authentication Services*, 15 (Jan. 29, 2003), *at* http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf (last visited Nov. 22, 2004) [hereinafter Article 29].

To streamline the communication of Passport-related regulations to clients, the Working Document also suggested the following: that Microsoft make clear that subscription to a Hotmail account would allow the exploitation of personal data to generate client-specific advertisements; that Microsoft make manifestly clear that it has no control over the privacy policies of participating sites; and that Microsoft provide special protection to EU Passport subscribers by notifying clients of relevant EU protection law when registering an account.[59]

Finally, to research potential technical solutions to the protection issues presented by Passport, the *Working Document* suggested that Microsoft "explore alternative architecture for .NET Passport" that would avoid assigning users unique identifiers (PUIDS), and separate account formation from storage of personal data in a profile, allowing for a new field by field flow of the information between the participating sites, and thus avoiding collection of excessive profile data.[60]

10. A MICROSOFT-MODIFIED POLICY ON PASSPORT

An indication of Microsoft's obligation to improve Passport, the fourth document to come out of the settlement agreements—Microsoft's new privacy policy on Passport utilization—established a higher standard of protection than had ever been expected by the Working Party. The modified Passport privacy policy reads:

> [participating sites] can use Passport profile information only to deliver the products and services requested by users. [Participating sites] cannot use Passport profile information to contact users for any purpose without obtaining the user's prior consent...cannot assign, transfer, share, transmit, or publicly disclose Passport profile information—or any identifiable information gathered from Passport profile—to any third party without the [client's] consent.[61]

---

[59] *Id.* at 6-7.

[60] *Id.* at 8-10.

[61] *Review Guide, supra* note 11, at 19.

II. .NET PASSPORT LESSONS FOR THE FUTURE OF UNIVERSAL ONLINE AUTHENTICATION

For several reasons, the Passport controversy is a significant landmark for online authentication architectures worldwide. The provisions of the *Working Document* appear to have impacted Microsoft clients worldwide—regardless of protection practices in their own countries. Even more amazing, in addition to avowedly following Party-specified privacy standards, Microsoft's modified privacy policy expanded on Party recommendations and further established privacy-promoting rules to which participating sites worldwide must now adhere.[62] And note the irony: when all is said and done, Microsoft, which at the outset had aggressively defied the EU's self-asserted extraterritorial jurisdiction, has introduced and implemented modifications that benefit clients worldwide—manifestly beyond the borders of Europe.

1. IS THERE A GENUINE REASON FOR UNIVERSAL SINGLE-SIGN-IN ONLINE AUTHENTICATION?

In their investigation, neither the Working Party nor the FTC evaluated the value of a single sign-on system *per se*. We noted above the many difficulties for which Passport was intended to be a solution. We then summarized—albeit briefly—the program's basic structure and features. From there, we outlined the argument advanced by various different organizations—led by EPIC—that these features violated cardinal privacy rights articulated in the letter of the law. In formulating an offensive, the organizations filed complaint petitions with the Working Party and the FTC, requesting that they halt distinct features and elements of Passport that allegedly ran counter to privacy rights. From then on, neither the FTC nor the EU ever thought to call into question the need for a universal single-sign in mechanism. Is there a genuine need for Passport-esque devices on the Internet? That is, could the difficulties that Passport was intended to solve be amended by other, presumptively more privacy-consonant, mechanisms? Even if the reply is an emphatic "no," so that Passport is the only viable solution in the market, did the difficulties truly merit a privacy-speculative and high-risk venture such as Passport? A balancing-test analysis was never performed. Why? What would be

---

[62] *See id.* (no distinctions between the privacy policies for EU and non-EU countries are observed).

the outcome? These are all questions amenable to further scholarship on the subject. Consonant with the previous line of questions, some privacy advocates feel that the Passport approach to authentication should be condemned, not improved.

In collaboration with various NGOs and websites, the Center for Democracy and Technology (CDT) has created what are called the Privacy Principles for Authentication Systems.[63] A key principle proposed by the group concerns the diversity of services and suggests that clients should have a choice about which authentication mechanism and providers to use, effectively opposing Microsoft's desire to create a universal, catch-all sign-on service.[64] EPIC, the leader in anti-Passport investigation in the U.S., agrees: although the modifications undertaken by Microsoft were "a step in the right direction," EPIC feels that the underlying issues have been neglected.[65] Additionally, EPIC contends that less risk is involved when clients store passwords in encrypted files on their personal computers—an alternative solution to the difficulties for which Passport was initially created. Lastly and somewhat ironically, EPIC believes that cutting-edge authentication system technology, such as Passport, "moves us backwards hundreds of years to barter-style sale arrangements where information is necessary to complete a sale."[66] Personal information is not necessary to purchase milk at the local food market. The Internet marketplace does not have to be any different.

2. PARTICIPANT SITE DISSATISFACTION WITH THE PASSPORT OUTCOME

Participant sites ("participants") also appear to be dissatisfied with the Passport case and its outcome. Without any knowledge of what Microsoft planned to do with previously-stored data on which they relied for business, participants were forced by the Passport case to halt site development and expansion until the settlements were

---

[63] Authentication Privacy Principles Working Group, *supra* note 3.

[64] *Id.*

[65] EPIC, *FAQ on Microsoft Passport and Windows XP, at* http://www.epic.org/privacy/consumer/microsoft/#faq (last visited Nov. 22, 2004).

[66] EPIC, *Project Liberty, at* http://www.epic.org/privacy/authentication/projectliberty.html (last visited Nov. 22, 2004).

concluded.[67] Second, EU restrictions left questionable incentive for participants to remain invested in Passport: in addition to a Microsoft licensing fee, European participants in the post-settlement era must conform to higher and more costly privacy standards.[68] Because the post-settlement Passport architecture allows the creation of multiple accounts for one client, the incidence of forgotten usernames and passwords has increased—a crucial problem for which Passport was founded in the first place. The ability to create multiple accounts has further decreased any marketing reliability Microsoft may have been able to provide to participating sites. Bashing the modified Passport scheme, Hal Stern of Sun Microsystems, a rival of Microsoft, joked: "If I sign up to Hotmail, forget my password and sign in again, I am suddenly two people according to Microsoft."[69]

In the post-settlement era, there remain crucial and meaningful questions as to whether the FTC and the EU Working Party actually brought about the modifications introduced to Passport. From beginning to end, neither agency ever thought to call into question the need for a universal single-sign in mechanism in the first place—whether a legitimate need for Passport-type devices on the Internet ever existed. That is to say, key underlying and rudimentary questions went unasked and unresolved. And now, in the post-settlement era, participant sites no longer see a reason to invest in Passport. Do the settlements provide *any* reason to celebrate?

Note that in 2002, research confirmed that the single sign-on authentication technology was no longer booming—a Gartner study estimated that there were 50 million registered authentication users (in contrast to the coinciding 250 million figure quoted by Microsoft).[70] By 2003, the study continued, the majority of those 50 million users would visit about three sites a month using the single sign-on service.[71]

Were the Passport scheme completely disfavored, the market would fall back into the initial difficulties presented at the beginning:

---

[67] VNU Business Publications, *EU Ruling Alters Passport*, Feb. 3, 2003, *at* http://www.infomaticsonline.co.uk/news/1138435 (last visited Dec. 14, 2004).

[68] *Id.*

[69] Jeanne-Vida Douglas, *Sun Responds to Mundie's Liberty Slur*, TECH UPDATE, Mar. 15, 2002, *at* http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2855454,00.html (last visited Nov. 22, 2004).

[70] Wilcox, *supra* note 14.

[71] *Id.*

sites want efficient authentication mechanisms and clients disfavor variant passwords. Perhaps this situation would yield a serious discussion about the one underlying question we feel has been neglected: what other ways are there to fix these difficulties? Sadly, we are not very optimistic: following Passport's lead, others have begun to incorporate the single sign-on scheme. The most notable of these is the "Liberty Alliance Project," launched in December 2001 as a contract-based group.[72] Comprised of more than 100 companies, non-profit organizations and governments worldwide, the Project's mission is to simplify sign-on through a "federated network identity."[73] In its investigation of Passport, the Working Party examined the Project and its development, concluding that it was neutral with respect to data protection.[74] For privacy advocates, the Project is far superior to Passport, mainly because the Project uses what are known as pair-wise identities—and not PUIDs—for each client.[75] The Project uses a username and password, but allows client data to be shared on a maximum of two sites.[76] Unlike Passport, the Project does not centralize client data; rather, client data is collected and stored by individual participating sites.[77] A user may federate his account to two service providers.[78] Account federation is used to enable users to link or terminate accounts.[79]

The Project is in its preliminary stages, and it is too early to assess its impact on the online community.

3. THE FUTURE OF ONLINE AUTHENTICATION IN GENERAL

As the authentication systems penetrate more and more into the heart of the internet community, it is important to ensure that these applications are designed to meet the basic data protection interests. It

---

[72] Article 29, *supra* note 58, at 11-13.

[73] *Id.* at 11-12.

[74] *Id.* at 12.

[75] *Id.* at 12-14.

[76] *Id.*

[77] Article 29, *supra* note 58, at 12-14.

[78] *Id.* at 4.

[79] *Id.* at n.13.

is important, therefore, to ensure that these systems meet some baseline standard of protection. The recommendations of the Working Party's *Working Document* can provide authoritative guidance in establishing such baseline standards. Thus, the authentication tools should aim to (a) hold the individual sites responsible for their data processing practices; (b) establish clear-cut and explicit contractual obligations between authentication providers and participants; (c) ensure minimal collection of client information; (d) to the greatest extent possible, provide clients with a possibility to employ anonymous or pseudonymous authentication; (e) facilitate the provision of full disclosure by the sites of their data protection practices to their clients; (f) employ minimum centralization in storing data; (g) allow clients maximum control over their data, including a possibility to modify and delete the same; and (h) ensure readily available procedures for handling client inquiries and complaints.[80]

The key issue in developing a protection-friendly authentication scheme is that authentication should not be equalized with identification—that is to say, there must be a way to authorize and authenticate site-client transactions without demanding a client's personal information. The EU Working Party *Working Document* reads: "[t]he use of identifiers, whatever form they take, entails data protection risks. Full consideration should be given to all possible alternatives."[81]

EPIC builds on this idea: in the best-case scenario, it argues that authentication should be anonymous. Again, optimal authentication would be similar to run-of-the-mill cash transactions; aside from the cash itself, no other credentials should be necessary to complete a transaction. In cases where anonymity is not an option, clients should be able to choose what personal attribute to provide for authentication. In that case, authentication involves selective disclosure of client information for verification — client identity is not disclosed.[82]

The online merchants should benefit from non-identifying authentication schemes, where such schemes are applicable, along with the privacy advocates. In the online community, where less than ten percent of customers are willing to exchange personal information

---

[80] *Id.* at 14-15.

[81] *Id.* at 15.

[82] Privacy International, *Privacy and Human Rights 2003: Threats to Privacy*, *at* http://www.privacyinternational.org/survey/phr2003/threats.htm (last visited Dec. 14, 2004).

in order to use personalized site services,[83] it is highly questionable whether the merchants' investments into deployment and maintenance of identification-based authentication tools would be able to yield adequate returns. Client identification should be required only when it is absolutely necessary, and research should be geared towards achieving that end.

4. THE IMPACT OF CROSS-BORDER COMMUNICATION ON THE FUTURE OF AUTHENTICATION

When creating a law of authentication systems, the formulation of the fundamentals—principles, concepts, and philosophies—on which that law is grounded are important. Equally important are the external factors outside of the law, which affect it regardless of these fundamentals. One can imagine a set of free-standing, internally-coherent, and logical principles as the founding layer of a law of authentication systems. The external factors, whether they are logical or unreasonable, coherent or messy, have to be taken into consideration. A case in point is Passport. The several investigations surrounding Passport gave rise to a discussion about fundamental principles, concepts, and philosophies—data decentralization, anonymity maximization, and market diversity—that had to comport with unavoidable external factors, such as the EU and U.S. legal orders, with which they were interacting. The international scope in which some laws operate, as in the Passport case, are of extreme importance and yield interesting consequences.

In the Passport case, the redevelopment of an American-produced product—Passport—anchored on EU law. Of the many changes implemented by Microsoft, only one was intended for the Europeans specifically: namely, the *required* creation of a prompt box that would "provide adequate information to the users concerning the data protection implications of the system."[84] The many remaining modifications, though suggested by the EU Working Party's *Working Document*, were directed at the whole world. Similarly, though the Working Party did not require that Microsoft dictate a privacy policy to participant sites, the modified Passport privacy policy requires that participating sites abide by EU-based principles.

---

[83] Wilcox, *supra* note 14.

[84] Article 29, *supra* note 58, at 15.

It is fascinating that an EU-dictated document written explicitly for the protection of its member states could have so monumental an impact on the rest of the world. As Mike Pullen, a data protection lawyer, remarked to the press: "'[t]here has been the opinion [in the US] that data protection in Europe does not have to be taken seriously - but now companies are paying attention.'"[85] An interesting consequence of the Passport case, which may appear in other circumstances in the future, is that when dealing with different regimes in the international arena, the regime that calls for the most rigorous modification—here, the EU—often affects authorities and peoples beyond its borders for economic reasons. This is because the involved party (like Microsoft) may either process all business transactions in a way that reflects the stringent approach (here the EU protection approach) or otherwise bear the extra cost of developing a subsidiary business model designed specifically for EU-related transactions.

But not everyone in the U.S. shares Pullen's excitement when it comes to the ubiquity of European protection law: "[t]he Directive in effect forces the United States, along with all other non-EU countries, to abide by its regulations...."[86] Evidence indicates that both the EU and the U.S. contributed to reshaping one another's laws, and that protection law has not expanded in one way only. The commodity approach embraced by the U.S. has penetrated into the EU. The Working Party did not ask Microsoft to terminate its direction of unsolicited advertisements to its Hotmail users. The Working Party felt and agreed that advertisements were a part of the business model, from which Microsoft was able to pull profits and provide the service free-of-charge.[87]

---

[85] David Neal, *EU Clamps Down on Passport*, VNU Business Publications, Feb. 10, 2003, at http://www.crn.vnunet.com/analysis/1138643 (last accessed Nov. 24, 2004).

[86] Julia M. Fromholz, *The European Union Data Privacy Directive,* 15 BERKELEY TECH. L.J. 461, 474 (2000).

[87] Article 29, *supra* note 58, at 7.

5. CHALLENGES AND VALUES OF INTERNATIONAL COOPERATION IN QUEST OF THE "GOLDEN BALANCE" BETWEEN COMPETING INTERESTS OF INTERNET USERS

In addressing Internet controversies, nations have two options. They may cooperate and collaborate—even in light of vast jurisprudential differences. Alternatively, they can implement conflicting laws, effectively creating more controversies without resolving the ones that have come before them. Fortunately, the Passport case exemplified and reinforced the idea of international cooperation; the Working Party and the FTC complemented one another's investigations and findings. The FTC voiced no objections to modified Passport policies brought forth by the EU. Moreover, though concerned about the security of the software behind Passport, the Working Party imposed no special security enhancement requirements on Microsoft, trusting "that Microsoft [would] put in place an Information Security Program in the framework of the Consent Order issued" by the FTC.[88] EU Internal Market commissioner Fritz Bolkestein expressed strong confidence in his collaboration with the FTC, stating:

> The Commission has regular contacts with the FTC on a wide range of issues....The Commission agrees that the FTC resolution is indeed an important step in the right direction. Although the FTC operates in a different legal framework than the one existing in Europe, the Commission has a positive opinion of the effectiveness of its enforcement actions.[89]

Further evidence of cooperation-induced success is that the Working Party's findings on Passport were mere persuasive authority—and at most international "soft law." The language that the *Working Document* incorporated lacked force and executive authority—it used "shall" instead of "should," and phrases such as "would be appreciated and encouraged." No enforcement mechanism

---

[88] Article 29, *supra* note 58, at 11.

[89] Written Question E-2439/02 of Erik Meijer, 2003 OJ (C 28 E) 0239-0241 (Aug. 28, 2002), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/ce028/ce02820030206en02390241.pdf (last visited Apr. 6, 2005).

was attached to non-compliance, save for a vague promise to continue monitoring Passport's deployment. Even the title of the Document—the *Working Document*—suggested powerlessness and a lack of binding demands; it is not an "Order," a "Judgment," or even an "Instruction." Thus there is reason to believe that the outcome of the case may have differed were it not for the FTC's enforcement powers.

The Working Party had two choices: it could demand sanctions from the Commission assigned to address Passport's problems, or sit idle and pray that Microsoft would abide by its provisions voluntarily. Though formally irrelevant to the enforcement of the Working Party's resolution, the FTC's participation created pressure on Microsoft to do its best in improving Passport. In contrast to the powerless language of the *Working Document*, the FTC's Consent Order is demanding and explicit. It provides concrete "shall" obligations. In lieu of a vague promise to "monitor" the issue should its recommendations not be followed, the Order unambiguously demands that Microsoft disclose and report relevant information to authorities, with a risk of penalty for failure to do so. One must not forget, however, that the scope of the FTC Order was restricted to addressing only deceptive misrepresentation practices. It did not intend to formulate universal standards for the authentication system industry, as had the *Working Document*.

In assessing the interaction between EU protection authorities and the FTC, Microsoft Senior Vice-President and General Counsel Brad Smith concluded:

> Consistent with our heightened security obligations, we accept responsibility for the past and will focus on living up to this high level of responsibility in the future....Industry and government will be most successful in promoting and protecting online security and privacy if these efforts are grounded in dialog and cooperation.[90]

III. CONCLUSION

At present, the proliferation of online authentication systems counter commonly-held ideas of privacy with respect to personal

---

[90] Microsoft, *Q & A: Microsoft's Agreement with the Federal Trade Commission on Passport, at* http://www.microsoft.com/presspass/features/2002/aug02/08-08passport.asp (last visited Nov. 22, 2004).

information. Given the international nature of the Internet, finding a balance between the value we place on authentication and the value we place on protection must accomplish two feats at once: achieving universal compatibility and appealing to the various legal frameworks (and the philosophies from which they arise) in the world. Though harmonization, maybe even unification, of internet law on an international level is unlikely to take place any time soon, the Internet naturally prompts international cooperation and collaboration between governments in resolving issues that arise—such as the Passport case.

For the foregoing reasons, and in light of the Passport case, future developers of authentication systems should adhere to the following guiding principles: 1) separate authentication from identification by providing anonymous authentication when possible; 2) minimize the collection of personal data; 3) minimize the centralization of data storage; and 4) maximize client control over corresponding data. To make sure that no existing authentication system usurps too much power over client data, it is vitally important that governments encourage and promote competition in the authentication system industry. As Passport developers have put it, "[m]aking computing safer and more trustworthy is a continuing challenge because consumers want both privacy and convenience – and those values can easily conflict."[91] Placed in the context of international relations, the task becomes even more difficult. But finding a mechanism that meets both demands—protection and convenience—in the international arena is the only way in which sites will be able to retain and expand their client bases. The "net" in "Internet" should not come from "trapping" personal information, but from offering the advantages of informed and secure "networking."

---

[91] Microsoft, *Q&A: Microsoft Passport Protects Consumer Privacy*, *at* http://www.microsoft.com/presspass/Features/2001/Aug01/08-12passport.asp (last visited on Aug. 12, 2001).