Before the
Federal Trade Commission
Washington, D.C. 20580

In the Matter of	)	
	)	**FTC File No. 0123240, M03**
Microsoft Consent Order	)	

To: The Commission

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC); U.S. PUBLIC INTEREST RESEARCH GROUP; REMAR SUTTON, PRESIDENT, THE CONSUMER TASK FORCE FOR AUTOMOTIVE ISSUES; JUNKBUSTERS CORP; COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY; PRIVACY INTERNATIONAL; CONSUMERS UNION; CENTER FOR DIGITAL DEMOCRACY; PRIVACY RIGHTS CLEARINGHOUSE; AND THE MEDIA ACCESS PROJECT.
September 9, 2002

Pursuant to the notice[1] published by the Federal Trade Commission on August 8, 2002 regarding the Consent Order entered into by the Microsoft Corporation and the Commission, EPIC; U.S. Public Interest Research Group (U.S. PIRG); Remar Sutton, President, The Consumer Task Force For Automotive Issues; Junkbusters Corp; Computer Professionals for Social Responsibility; Privacy International; Consumers Union; Center for Digital Democracy; Privacy Rights Clearinghouse and the Media Access Project submit the following comments.

We commend the Commission for taking action in this case. The Consent Order negotiated by the Commission broadly requires that Microsoft, through any authentication system offered in the future, build in protections for the use of personal information, including e-mail addresses, persistent identifiers in cookies, and identifiers that are embedded in hardware. Microsoft must fully disclose its information collection and use practices. Microsoft must develop a comprehensive security program that incorporates administrative, technical, and physical safeguards. Microsoft must obtain third-party review of its security program. Microsoft must maintain its public relations and marketing materials of Passport for Commission review. Microsoft and its successors must comply with these requirements for twenty years.

We believe that the Consent Order will go far in improving security and privacy practices associated with the Microsoft Passport Service. However, privacy hazards continue to remain in the Passport system.[2] Since we filed our original complaint in July 2001, there have been a series of security breaches at Microsoft, some of which involved Passport services.[3] Additionally, a recent Gartner study found that consumers are resistant to authentication systems,

---

[1] *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises*, Aug. 8, 2002, at http://www.ftc.gov/opa/2002/08/microsoft.htm.

[2] EPIC maintains a comprehensive page devoted to risks and security problems inherent in the Passport system online at http://www.epic.org/privacy/consumer/microsoft/.

[3] Most recently, a flaw in Windows XP, Office 2000, and other Microsoft products could enable a malicious actor to use a webpage or e-mail to send commands to a user's computer. *Microsoft Warns About Security Holes*, BBC News, Aug. 23, 2002, at http://news.bbc.co.uk/1/hi/technology/2211571.stm.

and that a majority of Passport users enrolled simply because Passport was necessary for access to some other service.[4] Despite these facts, Microsoft has attempted to expand Passport into an authentication system for credit card purchases,[5] and government entities have considered using Passport as an authentication agent for e-gov services.[6]

To ensure effective implementation of the Consent Order, we make four recommendations:

First, we recommend that since the intent of the Commission is to protect consumers from unfair and deceptive practices, the Commission should modify the consent order so as to require more transparency from Microsoft. Additional transparency is needed to ensure that consumers have adequate information about security and privacy risks in the Passport system.

Second, we recommend that the Commission examine authentication systems that are deployed and under development.

Third, we recommend that the Commission ensure that Microsoft is complying with the EU-US Safe Harbor, and that specifically, access to the entire Passport profile for correction and deletion is possible.

Last, we call upon the Commission to strengthen the security program for Microsoft by limiting the Passport system. Without limitations on the functions that Passport performs and the information that Passport collects, Passport becomes an increasingly attractive and lucrative target for malicious crackers.

I. Effective Implementation Requires Greater Transparency.

To ensure effective implementation, transparency is needed so that individuals and public policy makers can evaluate Microsoft's commitment to privacy and security. The FTC Consent Order requires Microsoft to engage in biannual assessments certifying the company's security program. We recommend that this report be made public for review. Without a publicly available report, individuals will not be able to evaluate Microsoft's representations regarding privacy and security. Specifically, the Commission should add language in section III of the Consent Order to read: "The report required by this paragraph should be available to the public by request, and online via prominent links on the Microsoft Passport website."

Further, we commend the FTC for requiring the report to be made by "a qualified, objective, independent third-party professional."[7] It should be noted that during the investigation, Truste

---

[4] *Study: Users aren't buying online ID hype*, ZDNet News, Apr. 25, 2002, at http://zdnet.com.com/2100-1105-892838.html; *Gartner Survey Shows More Internet Users Signing Up for Microsoft Passport, But Mostly to Get Other Offerings*, Gartner Press Release, Apr. 17, 2002, at http://www4.gartner.com/5_about/press_releases/2002_04/pr20020417a.jsp; *Web Users Pass On Passport-Style ID Services - Gartner*, Newsbytes, Dec. 4, 2001.

[5] *MS Passport Takes on Credit Cards*, ZDNet, July 8, 2002, at http://zdnet.com.com/2100-1106-942344.html.

[6] *Feds might use Microsoft product for online ID*, Seattle Times, Apr. 18, 2002, at http://seattletimes.nwsource.com/html/businesstechnology/134438173_passport18.html.

[7] In the Matter of Microsoft Corporation, No. 0123240 (2002) (agreement containing consent order at 4).

certified Microsoft's privacy policies.[8] Microsoft is a corporate sponsor of Truste, and has membership on the organization's board of directors.[9] Because of the relationship between Microsoft and Truste, and because Truste certified a privacy policy that was found to have contained material misrepresentations, we recommend that Microsoft be required to employ a different company to conduct the assessment and report. For purposes of performing the assessment, we believe that Truste fails to meet the "objective" and "independent" criteria set forth in the Consent Order.

Also consistent with principles of transparency, Microsoft should make available to Passport account holders their entire profile. Access should include the ability to view and correct information provided by the user, information collected by the system (such as authentication logs), and information that is acquired to enhance users' profiles. Specifically, we recommend that the Commission add a section to the Consent Order requiring that: "Microsoft shall provide to users access to their full Passport profile for inspection, correction, and deletion. Accessible information should include user-submitted information, access logs or other information automatically associated with an individual's Passport, and information that Microsoft uses to enhance Passport profiles."[10]

It is important that users of Microsoft XP or other Microsoft products be notified that a Passport is not necessary to access the Internet. Representations programmed into the Windows XP registration process are likely to lead individuals into believing that a Passport is necessary for accessing the Internet. We recommend in order to ensure effective compliance, and to maximize the value of notice to individuals, that Microsoft state clearly that a Passport is an optional service not necessary for Internet use. Specifically, we recommend that the Commission add a subsection to section I prohibiting Microsoft from misrepresenting in any manner, expressly or by implication, "whether enrollment in Passport is necessary to access the Internet or Internet-related services."

II. The Commission Should Examine Other Online Authentication Systems.

While Microsoft Passport was the focus of this investigation, we recommend that the Commission examine other authentication systems currently in development. As noted above, Consumers have been resistant to online authentication systems. However, companies with business models dependent on the exploitation of individuals' personal data continue to develop the systems and urge users to enroll, despite public resistance.[11]

---

[8] The FTC has granted Truste COPPA Safe Harbor Status. *TRUSTe Earns "Safe Harbor" Status*, FTC, May 23, 2001, at http://www.ftc.gov/opa/2001/05/truste.htm.

[9] Truste Sponsors, at http://www.truste.org/about/truste/about_sponsors.html; About Our Board of Directors, Truste, at http://www.truste.org/about/truste/about_purcell.html.

[10] In a recent settlement with the New York Attorney General, the online profiling company DoubleClick agreed to develop a "cookie analyzer" that will allow users to view their profile. *Major Online Advertiser Agrees to Privacy Standards for Online Tracking*, New York Attorney General, Aug. 26, 2002, at http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html.

[11] *See also Personalization? No thanks.*, Harvard Business Review, Apr. 1, 2002, at http://harvardbusinessonline.hbsp.harvard.edu/b01/en/common/item_detail.jhtml?id=F0104E.

America Online has launched the "Screen Name Service," which tracks users using personally identifiable information.[12] Users of the newly released Netscape 7 browser are urged to enroll in AOL's Screen Name Service, which employs prompts for personal information that are similar to the tactics used in the Windows XP operating system. Upon installation of the new browser, Netscape users are urged to create a screenname. The registration dialog box does not indicate that creating a screenname is optional. The dialog box only gives two options: "next" and "cancel." Individuals may be misled by these options, believing that selecting "cancel" will result in rending the browser inoperable. Individuals who enroll in the Screen Name Service are required to share personal information, including name, e-mail address, sex, date of birth, country, and zip code.

"Project Liberty" is an online identification and authentication system that is being developed by a consortium of companies.[13] It is similar to the Microsoft Passport system in that it allows individuals to use a single signon in order to access many different web pages.[14]

Authentication systems enable profiling, which results in more spam, direct mail, and telemarketing for individuals. Project Liberty has a stated goal of profiling individuals. The Liberty Alliance web page claims that the service is designed to: "Enable commercial and noncommercial organizations to realize new revenue and cost saving opportunities that economically leverage their relationships with customers, business partners, and employees."[15] The phrase "leverage their relationships" is a euphemism for secondary use of personal information for new forms of marketing and profiling.

Both AOL's Screen Name Service and Project Liberty present the same privacy hazards as Microsoft Passport. Accordingly, we recommend that the Commission examine these systems, and that the Consent Order set a minimum standard for privacy protection for these deployed and developed authentication systems.

III. The EU-US Safe Harbor Agreement Requires Access to the Entire Passport Profile.

Microsoft self-certified its compliance with the Safe Harbor Privacy Principles and intention to join the Safe Harbor on June 29, 2001.[16] The Safe Harbor Privacy Principles require that U.S. organizations seeking the protection of the Safe Harbor agree to follow certain doctrines of personal privacy protection in seven areas. Access to the entire Passport profile is required under the EU-US Safe Harbor Principles. The principles require a right of access for correction or deletion.[17] Currently, individuals have access to self-reported information in the Passport

---

[12] Screen Name Service, at http://my.screenname.aol.com/; *AOL Quietly Launches "Magic Carpet,"* Eweek, Jan. 14, 2002, at http://www.eweek.com/article2/0,3959,113131,00.asp.

[13] Project Liberty, at http://projectliberty.org/.

[14] EPIC maintains a webpage with information on Project Liberty online at http://www.epic.org/privacy/authentication/projectliberty.html.

[15] Liberty Alliance Project Q&A, at http://www.projectliberty.org/faqs/index.html.

[16] U.S. Department of Commerce, Safe Harbor List, at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

[17] Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access

profile, but they do not have access to authentication or other logs that build profiles on Passport users. Accordingly, we recommend that the FTC should require Microsoft to provide access to profiles under the Safe Harbor to European Union citizens.

IV. Effective Implementation of the Security Program Requires Limitations on Passport.

The security weaknesses of a single signon identification and authentication protocol have been well documented.[18] These weaknesses have also been demonstrated in a series of security breaches that threatened users' computers and their personal information. We believe that these security breaches will continue to occur, and accordingly, a security program for Passport must minimize the damage to individuals that these breaches will cause.[19] The harm from these security breaches could be mitigated if Microsoft developed genuine Privacy Enhancing Technologies (PETs)—tools that limit or stop the collection of personal information. Since Microsoft has adopted a profiling business model that depends on the collection of personal information instead, the Commission should require the company to develop a security program that mitigates risks to Passport users.

In the area of authentication, less harm would result from security breaches if Microsoft limited the functions that Passport serves. Currently, Passport is the functional equivalent of using a single key for one's house, car, and safe deposit box. As Passport serves more functions, it becomes a more attractive and more lucrative target for malicious crackers.

Microsoft has relied on a business model that requires personal information for unnecessary purposes, such as simply logging in on a website. Since the company requires individuals to reveal their personal information for access to services, the Commission should limit the functions that Passport serves and limit the amount of information the service collects in order to maximize the effectiveness of the security program. We recommend adding a section to the Consent Order specifying that: "Microsoft shall minimize requirements for authentication. Where Microsoft requires authentication, the company shall state the reasons for which authentication is necessary."

Risk of privacy violations would also be mitigated if the Passport system accepted pseudonymous or anonymous authentication. A Passport that contains less personal information carries with it a diminished risk to the individual. Currently, a fully populated Passport

---

would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. Safe Harbor Principles, 65 Fed. Reg. at 45,668.

[18] Chris Shiflett, *Passport Hacking Revisited*, Aug.15, 2002, at http://shiflett.org/articles/passport_hacking_revisited/; *Microsoft Passport Hijack Attack*, Eye on Security, July 23, 2002, at http://eyeonsecurity.net/papers/passporthijack.html; Chris Shiflett, *Passport Hacking*, 2600: The Hacker Quarterly 18.3 (2001): 11-13, at ; David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Signon Protocol*, Computer Networks, Elsevier Science Press, volume 33, pages 51-58, 2000, at http://avirubin.com/passport.html.

[19] At a recent .Net developer conference, a Microsoft Senior Vice President lamented, "We really haven't done everything we could to protect our customers...Our products just aren't engineered for security." *Lead Windows developer bugged by security*, Infoworld, Sept. 5, 2002, at http://www.infoworld.com/articles/hn/xml/02/09/05/020905hnmssecure.xml.

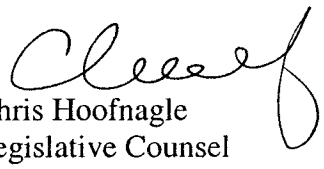
facilitates the sharing of name, e-mail address, date of birth, country, and zip code. Sharing this personal information puts the individual at greater risk for identity theft, as date of birth is often used as an authenticator for credit purposes. We recommend adding a section to the Consent Order that requires Microsoft to: "Incorporate techniques for anonymity and pseudoanonymity that would allow users of Passport to authenticate without revealing their true identity."

Individuals' privacy would be further protected if the security program required regular data destruction, so that the Passport database does not contain a comprehensive log of user authentications. We recommend adding a section to the Consent Order specifying that: "Individually-identifiable data collected by the Passport system shall be purged regularly. This shall include user data stored on back-up systems."

The security program would also be strengthened if the Commission closely monitored and remedied Microsoft's future security breaches.[20] We recommend that the Commission require Microsoft to notify the agency whenever a security breach results in an unauthorized transfer of personal information. Those affected by the security breach should also be promptly notified. Accordingly, we recommend adding a section to the Consent Order specifying that: "Microsoft shall notify the Commission as soon as practicably possible following a breach of security that results in user data being compromised. Microsoft shall also notify Passport holders affected by the breach."

Respectfully submitted,

Marc Rotenberg
Executive Director



Chris Hoofnagle
Legislative Counsel

Electronic Privacy Information Center
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009

[20] We note that increasingly, companies have been held liable for damages for their online security violations. The New York Attorney General has obtained monetary remedies from Ziff-Davis Publications and Eli Lilly in recent months because of unintentional privacy violations.