MICROSOFT AND THE EUROPEAN UNION FACE OFF OVER INTERNET PRIVACY CONCERNS

Amidst what appears to be a multi-faceted attack by the European Union on Microsoft, the newest angle is the European Commission's announcement last month that it was considering a formal investigation of Microsoft's .Net Passport data processing system for possible violations of the European Union Data Privacy Directive.[1] This iBrief explores the European Data Privacy Directive and seeks to explain why the European Commission believes .Net Passport may be in violation of its privacy policies and a case for further investigation.

The European Privacy Directive: An Overview

Basic Philosophies

The European Data Privacy Directive ("Directive") was formally adopted by the European Union ("EU") in 1995, and became effective in October 1998.[2] According to Article 1 of the legislation, the Directive has two primary objectives – to protect the fundamental right of privacy and promote the continued free flow of personal data between Member States.[3] Steven Salbu, in his article *The European Data Privacy Directive and International Relations*, notes that because of Europe's past experience with the "invasive data collection methods" of the Third Reich, "privacy considerations that may be considered negligible in the United States are taken very seriously by the European Union."[4]

In furtherance of protecting privacy as a fundamental right, the Directive incorporates a unique "opt-in" provision. As Salbu explains, "The 'opt-in' approach … presumes an expectation of data privacy as the default position."[5] This presumption derives from the Directive's mandate, in Article 7, that "personal data may be processed only if: (a) the data subject has unambiguously given his consent…"[6] As Fred Cate notes, in his article *The Changing Face of Privacy Protection in the European Union and the United States*, there are "protection of 'public interest' and 'legitimate interests' of a private party" exceptions to Article

---

[1] Reuters, *EU: MS Passport is under investigation* (2002), at http://zdnet.com.com/2100-1104-934916.html.
[2] Steven R. Salbu, *Regulation of Borderless High-Technology Economies: Managing Spillover Effects*, 3 CHI. J. INT'L L. 137, 137 (2002).
[3] *Council Directive 95/46/EC*, 1995 OJ (L 281), art. 1.
[4] Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 666 (2002).
[5] Salbu, *supra* note 2, at 137.

7; however, the Directive's overall position on the data subject's own privacy interest, is in direct conflict with the United States "opt-out" privacy mentality.[7] The EU Directive requires, in most cases, that data processors make it perfectly clear to the data subject that they want to collect and use the subject's personal data, and the subject must "unambiguously" consent to the data collection, use, storage, etc. By contrast, the U.S. "opt-out" presumption only requires that the data collector make available an option whereby the data subject can be removed from the data collection process.[8] To illustrate, data, such as names and telephone numbers, could not be used in the EU for unsolicited telemarketing without prior consent of the data subject to that collection and specific use of his or her personal data. Alternatively, in the US, one must ask to be removed from telemarketing list, thus opting out of the continuing data collection and use. Essentially, the EU Directive requires the data collectors to obtain consent from the data subject, whereas U.S. data collectors presume consent, and require an affirmative opt-out. This opt-out versus opt-in debate reflects a major philosophical difference in how the EU and U.S. regard personal data privacy, and it is an important distinction in the context of Microsoft .Net Passport, discussed *infra*.

In regard to the second objective, promoting the free flow of data among Member States, the Directive's preamble clearly explains that, in accordance with the EU's model of "economic and social integration, … difference[s] in levels of protection of the rights and freedoms of individuals" may in turn affect data privacy by "prevent[ing] the transmission of such data … between territories."[9] As a result, the Directive is designed to "coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner…"[10] These two objectives, protecting the fundamental right of privacy and designing a system that promotes territorial uniformity, are at the heart of the Directive.

Directive Implementation

The EU Member States are responsible for integrating the Directive into their own political and legal systems. First, it is important to note that the guidelines set out in the Directive

---

[6] *Council Directive*, *supra* note 3, at art. 7(a).
[7] Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 182 (1999).
[8] Jon Swartz and Byron Acohido, *EU scrutinizes Microsoft's Passport,* USA TODAY, June 12, 2002, at 3B.
[9] *Council Directive*, *supra* note 3, at pmbl. 5, 7.
[10] *Id.* at pmbl. 7.

are at most a minimum level of protection.[11] Member States use their own discretion in setting maximum margins in their subsequent national privacy legislation.[12] The baseline, according to Directive Article 3, requires Member States to implement legislation that regulates and protects "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[13] Article 2(a) defines "personal data" as "any information relating to an identified or identifiable natural person."[14] Further, "processing of personal data" includes "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage."[15] Finally, "personal data filing system" applies to "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis."[16] All of this translates into creating a data processing system that is theoretically "accurate, up-to-date, relevant, and [perhaps most importantly] not excessive."[17]

Directive Policy Toward Third-Party Data Transfers

The Directive's rules on third-party (non-EU-Member States) data transfers are often cited as highly controversial.[18] According to Directive Article 25, "Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if … the third country in question ensures an *adequate* level of protection" (emphasis added).[19] As Salbu notes, in connection with the definition of "processing of personal data," "[I]n reality, Article 25 would affect virtually all personal data transmissions."[20] Further, Article 25, § 2 provides that "adequate level of protection" is "assessed in the light of all the circumstances surrounding a data transfer operation or set of data operations."[21] While there are further guidelines, such as consideration of the nature of the data, purpose and duration of the data operation process, and country of origin and

---

[11] Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 468 (2000).
[12] *Id.*
[13] *Council Directive, supra* note 3, at art. 3(1).
[14] *Id.* at art. 2(a).
[15] *Id*. at art. 2(b).
[16] *Id.* at art. 2(c).
[17] Cate, *supra* note 7, at 182.
[18] Salbu, *supra* note 4, at 675.
[19] *Council Directive*, *supra* note 3, at art. 25(1).
[20] Salbu, *supra* note 4, at 675.

destination, the standard is still relatively subjective and vague.[22] It is also extremely far-reaching for both countries and corporations outside the European Union. As Cate explains, "Because of the difficulty of separating data collected within Europe from data collected elsewhere, the directive effectively requires multinational businesses to conform all of their data process activities to European law."[23] As another scholar observed, "The Directive in effect forces the United States, along with all other non-EU countries, to abide by its regulations, to negotiate with the EU in order to win an interpretation that is more flexible than the words of the Directive suggest, or to suffer the ill consequences of not being able to transfer data out of the EU."[24] This kind of data flow restriction could seriously frustrate transnational electronic commerce.[25]

If a non-Member State is adjudged under these guidelines and found "inadequate" in regard to level of data protection, then non-Member States do have the option of setting up "safe harbor" agreements to continue data processing in European Union States.[26] These provisional agreements set up guidelines, by which particular non-Member States (and thus corporations in that State) must abide in order to reach an adequate level of protection.[27] The safe harbor agreement essentially acts as a gap-filler to address what the European Commission views as inadequate privacy protection.[28] The U.S. Commerce Department negotiated its safe harbor agreement with the EU in July 2000.[29] Companies that wish to do data processing work, which is subject to the rules of the Directive, must agree and sign a commitment (with the Department of Commerce) to the terms of the safe harbor agreement.[30] The safe harbor option in Article 26 does provide minor relief to the Directive's strict policies, but non-Member States/corporations, even under safe harbor agreements, are still subject to the guidelines and interpretations dictated by the Directive and the European Union.

The EU Privacy Concerns Involving Microsoft's .Net Passport

The Situation

Microsoft's single sign-in web surfing system, .Net Passport, allows users to store personal data information, such as email account/user names, passwords, and purchasing

---

[21] *Council Directive*, *supra* note 3, at art. 25(2).
[22] *Id.*
[23] Cate, *supra* note 7, at 184.
[24] Fromholz, *supra* note 11, at 474.
[25] *Id.*
[26] *Council Directive*, *supra* note 3, at art. 26.
[27] Salbu, *supra* note 4, at 679.
[28] Fromholz, *supra* note 11, at 476.
[29] Salbu, *supra* note 4, at 670.
[30] Salbu, *supra* note 4, at 670.

information (including name, address, phone and credit card numbers), online for use on numerous affiliated websites.[31] Most .Net Passport users are automatically registered for .Net Passport when they open a Hotmail e-mail account, Microsoft's free online email service.[32] Microsoft's new Windows XP operating system also gives users the option to register with .Net Passport upon setting up their Internet connection.[33] In total, Microsoft estimates that it has more than 200 million Passport users worldwide.[34]

Microsoft's .Net Passport operations with users residing in the EU has drawn criticism from European national data controllers and privacy watchdog groups for some time,[35] but .Net Passport's data procedures reached the political forefront in late May when Dutch MEP Erik Meijer accused .Net Passport of having "surreptitiously passed (data) on to unknown parties."[36] Given what EC data-protection department head Sue Binns described as a "software [system] that collects personal data and redistributes it in a way which isn't very well controlled," the EC took these claims and other associated privacy concerns "very seriously" and launched a preliminary probe into the system.[37] Microsoft was quick to respond to these accusations, stating that .Net Passport was in compliance with the Directive, and that Microsoft was "in a 'constructive dialogue' over this issue with the Commission and the EU states."[38] Microsoft representatives also repeatedly emphasized that no EU Member State had formally launched an investigation into the matter.[39]

After an early July meeting, the EU had still not launched a formal investigation, but did expand their probe, according to what the EU Internet Task Force members called a "need for closer checks."[40] These checks include addressing concerns over whether .Net Passport users "were fully aware that some of their data would sometimes be transferred to a party other than Microsoft," if the "consent" was of the quality needed to satisfy the Directive demands, and whether there were still other security risks present in the system.[41] If the probe results in an

---

[31] Microsoft .Net Services Overview (2002), at http://www.microsoft.com/netservices/passport/overview.asp#record.
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] Swartz and Acohido, *supra* note 8, at 3B.
[36] Adrian Cox and James G. Neuger, *Microsoft's Passport Provokes EU Privacy Concerns, Binns Says,* BLOOMBERG NEWS, June 25, 2002.
[37] *Id.*
[38] Reuters, *supra* note 1.
[39] *Id.*
[40] Reuters, *EU Launches Probe into Passport Privacy* (2002), at http://zdnet.com.com/2100-1106-941248.html.
[41] *Id.*

investigation or an eventual ruling that .Net Passport is in violation of the privacy Directive, Microsoft would be fined and required to rework the .Net Passport system to satisfy the Directive or pull .Net Passport from use in EU markets.[42] Neither option is good for Microsoft. Reworking .Net Passport to satisfy the EU Directive could be a relatively costly venture for a specified market; and in a world where e-commerce is an increasingly favored option for both business and personal use, pulling .Net Passport from the EU market would inconvenience users and businesses alike.

The Specific Problem

As highlighted by the latest EC findings, Microsoft's .Net Passport problems revolve around user consent (or lack thereof). The concern over blind transfers to unidentified parties and adequacy of consent both result from questions as to whether users entered into the data processing (be it email addresses, credit card numbers, etc.) with full knowledge and understanding of what Microsoft would do with their data, including the possibility that their data could be passed to other unidentified parties.[43] This concern harkens back to the EU opt-in philosophy versus the U.S. opt-out presumption debate that governs these kinds of data transactions. If Microsoft is operating .Net Passport under the presumption that users opt-out of data processing, then it is not in compliance with the Directive. To be in line with the European Directive, Microsoft has to make its data processing conditions, such as locations, parties, use, length, and so on perfectly clear to its .Net Passport European users, and it must receive from its users an "unambiguous" agreement to its stated terms. Despite Microsoft's claims of compliance, if the EC comes back from its probe with a decision to launch a formal investigation, Microsoft undoubtedly will have to take a closer look at its "volunteered" information clause to see if it is truly an opt-in clause that is in compliance with the Directive or really just an American opt-out clause in European clothing.

Conclusion

This latest angle in the barrage of issues the European Union continues to find with Microsoft may not seem as important as ongoing anti-trust investigations, but it is still nevertheless very important for what it illustrates about the broad application of EU Directives to multi-national corporations, and even more fundamentally for what it says about two very different concepts of user privacy rights on the internet. Whatever one's thoughts may be on which system, opt-out versus opt-in, is more fair, the .Net Passport debate has shown the growing

[42] *Id.*

transnational world of commerce, particularly computer software giant Microsoft, that the wording next to the checked or unchecked consent box may be equally as important as the terms that precede it.

By: Seagrumn Smith

[43] *Id.*