

# Microsoft: Working with privacy regulators

**Peter Fleischer** explains how Microsoft's pro-active approach to working with the EU Article 29 Working Party has provided a valuable template for future dialogue on privacy issues.

The Internet benefits consumers in many ways, while simultaneously raising challenging data protection and privacy issues. Many of these issues are not clear-cut, as complex new technologies often cannot be analysed easily under data protection law. This article highlights one example of how, working together, Microsoft and the European Union's Article 29 Working Party examined the privacy aspects of a cutting-edge service – Microsoft Passport – and jointly developed a strategy that enhances the privacy of users and sets a model for other Internet services going forward.

We at Microsoft believe this example represents precisely the type of dynamic public/private dialogue that is necessary in today's fast-paced and high-tech global economy.

## AUTHENTICATION SERVICES AND PASSPORT

Passport is one of a new generation of "authentication services" that help users navigate the Internet. Authentication services were born of the simple fact that many Internet sites ask users to register and create an account. Unfortunately, users must frequently remember different usernames (and sometimes passwords) for different sites. Because these can be difficult to recall, users often compromise security by writing down their login information, or storing it on a computer to which others have access. Alternatively, users may forget their username and password for a particular site, and are unable to access their account, causing frustration and disappointment.

Passport offers a solution to these problems. It is a sign-in system that allows users to create a single username and password which are used to log into multiple Internet sites. This means that users need only to remember a single set of login credentials. In addition to simplifying logins at sites, Passport

allows users to store certain additional information – such as their name, country, birthday, etc. – in their Passport profile and elect to share it with participating sites. This helps ease registration, as users do not have to retype the same information at multiple sites.

## MICROSOFT'S DIALOGUE WITH THE WORKING PARTY

In the summer of 2002, the Working Party, which consists of representatives of all national data protection authorities in the EU, began considering the privacy ramifications of authentication services in general, and Passport in particular. In connection with its review of such systems, the Working Party contacted Microsoft. An eight-month discussion ensued, which the Working Party later described as a "very open and fruitful dialogue" (see notes). We discussed the Working Party's concerns, meeting in person, speaking by phone, and exchanging correspondence. Not surprisingly, these discussions were frequently very technical, as various ways of designing and programming authentication systems were evaluated from both a privacy and a commercial perspective.

The detailed and lengthy nature of these discussions brought home to all participants the challenges involved in applying data protection principles to new, evolving technologies. For this reason, our discussions included everyone from programmers to legal/regulatory specialists.

By involving many different people with different backgrounds, we were able to develop technical solutions that addressed the Working Party's concerns without sacrificing any of the underlying functionality that makes Passport so popular. And clearly, the discussions were successful. As the Working Party concluded: "[we] welcome the important steps that Microsoft has taken and

is going to take in the next months in order to ensure the compliance of the .NET Passport system with the European Data Protection Directive."

At Microsoft, we believe that the changes made to Passport set the bar for data protection on the Internet, in some important ways, as described below.

## COLLABORATIVE DEVELOPMENT OF TECHNICAL SOLUTIONS

Our discussions with the Working Party covered many different issues, ranging from the overall design of authentication systems, to the specific technical details of certain Passport functions. During this process, the following subjects proved particularly important:

**Information disclosure** - Microsoft and the Working Party both recognised that users must receive clear information about how data entered during the registration process will be used by Microsoft, as well as by participating sites, some of which are based in countries outside the EU. We therefore discussed and evaluated many different ways of communicating key privacy information to users.

Our shared goal was to provide users with sufficient privacy information to make an informed decision, without overloading them. Microsoft and the Working Party ultimately found that the best way to address this challenge is to present EU users with a hyperlink to a prompt box that gives key privacy information. The prompt box summarises in an easy, readable way, key information about Passport's privacy policies, and contains hyperlinks to more information about Passport's privacy practices.

**User control** - Passport provides authentication services to a number of participating Internet sites, some of which are outside the EU, and all of which have their own practices with

respect to handling of users' data.

Microsoft and the Working Party discussed various ways of ensuring that users retain control over use of their data by participating sites. To this end, participating sites will be required to indicate in what country they are established, and the prompt box described above includes a link to the European Commission's web page indicating which non-EEA countries have been found to have adequate data protection laws. Finally, Passport's registration page will eventually allow users to choose – on a site-by-site basis – precisely what information to share with participating sites, and even to change that information from site to site. In this way, users are given maximum information about how their data will be used, and maximum control over such use.

**Password selection** - Users tend to create overly simple passwords, focusing on ease of remembering rather than difficulty of cracking. Microsoft and the Working Party considered how best to encourage users to create stronger passwords that are harder to break. In the end, we both felt that the best approach is to provide users with real-time feedback on the strength of their password via a red-yellow-green meter, and include a hyperlink to a page containing additional information about creating strong passwords.

As noted above, this collaborative development of technical solutions helped alleviate many of the Working Party's concerns. Nevertheless, as the Working Party's report notes, two areas of concern remain. First, the Working Party was concerned by Passport's use of a unique identifier, fearing that such a number could be used by participating sites to build profiles about particular users. We discussed various alternatives with the Working Party, but noted that each of these systems carried with it particular privacy benefits and drawbacks and that none was clearly superior from a privacy perspective.

We also discussed whether users of a "free" Internet service should be able to opt-out of targeted advertising that funds the service without also losing the service. This issue is broader than just Microsoft, as it affects a basic economic model for offering Internet services, and

we and the Working Party agreed that it should therefore be addressed in a wider context involving all stakeholders.

#### THOUGHTS FOR THE FUTURE

Out of our experience with the Working Party, we see two developments of note. The first is the importance of open and cooperative dialogue. Increasingly, regulators are going to interact with technology, as they seek to protect citizens' rights. At the same time, new technical developments bring benefits to society, with an increased variety of services ever easier to access. We think that the process Microsoft engaged in with

fact that each of the Working Party members is a regulatory body in its own right, with enforcement powers. This development has the potential to be beneficial to both users and providers of services, as well as regulators. By working cooperatively through the Working Party, regulators and companies can avoid inconsistent application of data protection rules, allowing companies to offer the same services, in the same manner, throughout the EU while ensuring compliance with privacy rules and avoiding increased compliance costs and burdens resulting from inconsistent national regimes.

---

**cooperative dialogue is an efficient and effective means of addressing concerns that may arise with regulators, while ensuring that new products and services remain commercially attractive and feasible.**

---

the Working Party shows that cooperative dialogue is an efficient and effective means of addressing concerns that may arise with regulators, while ensuring that new products and services remain commercially attractive and feasible.

The second relates more specifically to the Working Party. Article 30 of the EU Data Protection Directive empowers the Working Party to study new issues, services and products, and report back to the Commission. However, in Passport and other contexts, it seems clear that the Working Party is moving beyond this role and beginning to act as an embryonic pan-European regulatory body. In some ways, this is a natural outgrowth of the

#### CONCLUSION

The rapid pace of technological growth will continue to raise new and challenging issues for both public officials and the private sector. We at Microsoft believe that these issues are best addressed through consultation and dialogue. Our extensive discussions with the Article 29 Working Party demonstrate clearly the benefits of such a consultative process, and we hope that this approach will be used as a template for future public/private dialogue. By working together in this way, government and industry can protect individual liberties and ensure that the benefits of the Information Society are fully realised throughout the EU.

---

*i*

---

**AUTHOR:** Peter Fleischer is Director of Regulatory Affairs, Microsoft EMEA. Based in Paris, he is responsible for all aspects of regulatory compliance, including data protection and privacy. He can be contacted at [peterfl@microsoft.com](mailto:peterfl@microsoft.com).

**FURTHER INFORMATION:** The Working Party has published two working documents relating to online authentication services: *First Orientations of the Article 29 Working Party concerning online authentication services* (WP60, July 2nd 2002); and *Working Document on online authentication services* (WP68, Jan 29th 2003). See: [http://europa.eu.int/comm/internal\\_market/privacy/workinggroup\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup_en.htm)

---