Case study: Enhancing information and network security – Cornelia Kutterer

Technological advances have great societal benefits and make it easier for people to access information, and to collaborate with their communities. They also expose users to risks such as cybercrime, identity theft or misuse of personal data. Software companies share a responsibility to design and operate products and services in a manner that both helps protect customers from these harms and promotes respect for fundamental rights. And software companies share, with many other stakeholders, a collective responsibility to help make the Internet more reliable and trustworthy. The steps appropriate for a software company to take, however, must recognize the appropriate role for private sector actors. Policy considerations regarding economic incentives must be borne in mind – the impact on innovation and competition of investing private actors with responsibility for public goods. Accountability is important as well – in many cases, steps are best undertaken by democratically elected governments rather than private actors, particularly actors with market power.

Finally, when striving towards these goals, public policy objectives such as governance, security, privacy and freedom of expression may sometimes seem at odds. That is why integrated processes in developing software as well cooperation and dialogue with all stakeholders is crucial to ensure fundamental rights and the safety of users.

Our Process and Practices

In the section below, we set out briefly our process and practices for integrating public policy objectives and ensuring stakeholder engagement in our decision-making. These practices focus on Microsoft's software businesses, rather than our online services businesses, though it must be borne in mind that the advent of 'cloud computing' - a priority focus for the Microsoft software business - means that the Internet and related policy issues play a still larger role in the software business than ever before.

Security Process

Microsoft integrates security best practices into the software development process. This process, the Security Development Lifecycle (SDL), adds well-defined security requirements and recommendations at appropriate points in the development process.1 Following these process steps helps development teams to reduce the quantity and severity of security bugs shipped to customers. We also take steps to ensure our software and services meet relevant security standards, and we have fashioned security response systems so that attacks or security issues are addressed quickly, and notices circulated appropriately.

Privacy by Design, Default and Deployment

We built and extended a similar process to ensure that privacy was incorporated into our products and services by default, design and deployment. We review a product or service based on level of privacy risk at the beginning of the design process, through implementation, through release to beta and finally public release. This standard, the Microsoft Privacy Standard for Development (MPSD) is part of the SDL process and includes detailed guidance on creating customer notification and consent procedures, providing sufficient data security features, maintaining data integrity, offering user access, and supplying controls when developing software products and Web sites.. As part of our commitment to sharing best practices with the technology industry and privacy community, Microsoft has released a public version of the MPSD: Privacy Guidelines for Developing Software Products and Services (http://go.microsoft.com/ ?linkid=9707862).

We also take steps to integrate respect for privacy into our work with governments to respond to subpoenas and other requests for user data. Illustrative of our approach are the Law Enforcement-Internet Service Provider guidelines published by the Council of Europe,3 which set out steps for effective cooperation that both addresses cybercrime and respect for fundamental rights.

We also have specific procedures to protect privacy in the context of free expression. This includes decision-making about the markets where such data will be stored. Before certain types of personal information can be hosted in a particular country, Microsoft undertakes a due diligence examination of the country concerned, including a review of its overall human rights situation and the rule of law.

Human Rights – Freedom of Expression

Freedom of expression is a human right and guarantor of human dignity. This right includes the freedom to seek and impart information of all kinds, and through any medium. Privacy, in addition to being a fundamental right in itself, is also an enabler of free expression – and preserving anonymity in appropriate contexts is an important policy objective.

We're pleased to have helped create the Global Network Initiative (www.globalnetworkinitiative.org), an organization dedicated to advancing Internet freedom, along with other leaders from industry, human rights organizations, academics, and socially responsible investors. The GNI principles and guidelines establish certain baselines that help guide us in addressing freedom of expression and privacy in information and communications technologies, and provides an important forum for stakeholder feedback and learning.