Roundtable for Privacy Enforcement Authorities and Privacy Professionals

27 May 2008, 9:30 – 17:30 OECD Headquarters, Paris

Summary of the Discussions

The Roundtable gathered some 50 participants, composed of privacy enforcement authorities and privacy professionals from many parts of the world. Canadian Privacy Commissioner Jennifer Stoddart chaired the day-long event. The agenda was oriented around four topics that were addressed through moderated panel discussions, and generated an active exchange among panellists and non-panellists alike.

The concluding session highlighted the value of the event and suggested that there would be interest and value in future roundtables to bring together privacy authorities and professionals in a similar roundtable format. Some **key themes** that emerged from the discussions include:

- Working together, authorities and professionals can help make the application of privacy laws more predictable for organisations and beneficial to individuals.

- Working towards a more strategic approach to complaints handling is important. The concept of harm could be further explored in this respect.

- Complexity is a challenge, both in terms of applying local laws to global operations, and understanding the privacy impacts of emerging technologies.

- The greater the complexity of compliance the more likely an organisation will take the risks of non-compliance.

- While harmonisation is desirable in principle, equivalencies or mutual recognition may be more practical alternatives.

- Greater attention to risk assessment and management as well as accountability tools can be beneficial.

- Governments could focus on better understanding the link between privacy and economic policy, as the scope and value of global information flows continue to increase.

Introductions

The Roundtable began with a session to introduce the participants to the key international forums oriented to authorities and professionals. For privacy authorities, the overviews covered the International Conference of Data Protection and Privacy Commissioners, the Article 29 Data Protection Working Party, and the Asia Pacific Privacy Authorities forum. These groups provide authorities with opportunities to exchange views about current challenges, good practices, and sometimes result in the expression of common opinions on privacy issues. These types of activities are also important within a purely domestic context, as was pointed out during a presentation of the situation in Japan, where enforcement responsibilities are distributed across a number of government ministries, rather than being housed in a single authority.

Private sector privacy professionals interact through a number of forums, several of which were represented at the Roundtable. These included the European Privacy Officers Forum, the European Privacy Officers Network, and the International Association of Privacy Professionals. It was noted there are quite a number of similar forums around the world, such as the German Association for Data Protection and Data Security. Each of these groups serves its members by providing opportunities for networking and exchanges of views and good practice on topical issues of shared concern. The professional networks also seek to facilitate contact between their members and privacy authorities. An emerging activity is the certification of privacy professionals.

1. Focusing on Privacy Priorities

The two morning panels considered how privacy authorities and professionals can assist one another in focusing their energies on the high priority activities. Both authorities and professionals face challenges related to limited resources, as well as coordinating efforts across borders -- increasingly a necessity in today’s global economy.

Streamlining Enforcement for Privacy Authorities

The first of the panels took the point of view of the authorities and a number of suggestions emerged on how to increase the efficiency and effectiveness of enforcement activities. Considerable attention was focused on the issue of complaints handling. Some authorities are obliged by law to investigate every compliant they receive, which puts a premium on having an efficient process in place to address complaints. One suggestion was for an authority to first try to have the complaint resolved by the company directly with the individual before expending resources to investigate. Other suggestions addressed how best to prioritise complaints. For example, greater resources could be devoted to complaints where the harm appears to be greatest.

It was pointed out that complaints can serve an important intelligence gathering function, providing authorities with indications of problems in particular sectors, or with particular organisations. The value of this information can be reduced, however, when authorities that are obligated to investigate all complaints try to reduce their burdens by discouraging the filing of complaints. It was also observed that while complaints can serve to indicate the existence and scope of a problem, the volume of privacy complaints in particular does not always correspond to the scope of the problem. Some complaints can be trivial, and others can be related more to education and public awareness than to the actual scope of the problem, as individuals are often unaware that their information has been misused. The lesson is that complaint data is not the only way to set priorities.

The need for authorities to find the right balance between enforcement and awareness raising was also highlighted. A number of other trends were discussed, including the recent increase in investigations and audits by authorities. Partnerships and joint training exercises were suggested as means for improving co-operation between authorities and professionals. In particular, partnerships between authorities and key industry associations (e.g. direct marketing, banking) can be useful.

The role of civil society was also discussed. For example, authorities can work with civil society representatives on awareness raising campaigns, taking advantage of the fact that civil society is often quite skilled in its dealings with the media. Further discussions with civil society may be useful on other issues, such as complaints handling and the obligation to investigate all complaints.

Streamlining Enforcement for Privacy Professionals

The second panel turned the focus to the challenges facing privacy professionals. The difficulties of operating globally in a world with local user expectations and privacy laws were frequently highlighted. Some attention was given to Binding Corporate Rules (BCRs), but it was pointed out that even BCRs face the obstacles of differing national requirements and processes. One particular topic raised was registration requirements related to data processing. It was noted that there are 29 different registration processes within the EU alone. Given the current flows of data, it was suggested that the limited numbers of registrations reported by authorities indicate considerable non-compliance with these registrations requirements. Some companies have appeared to be focusing on the risk of enforcement action in determining compliance levels. Some authorities in jurisdictions not requiring registration suggested that this absence did not appear to reduce the privacy protections enjoyed by their citizens. One participant offered this rule of thumb: for every compliance burden there should be a corresponding privacy benefit.

Other challenges discussed include the difficulty of interpreting and applying privacy laws to the complexities of current data processing practices. This is particularly the case for applying laws to processing practices involving new technologies, with behavioural targeting being cited as one example. Privacy officers serve important functions in terms of managing privacy risks and resolving disputes in this environment, but their roles should be clearly defined and they should not be expected to serve as whistleblowers or held personally accountable for all violations by their organisations.

2. Preventing Privacy Harms

The two panels of the afternoon session included both authorities and professionals. The overall focus of the sessions was efforts to prevent privacy harms from happening in the first place (rather than mechanisms for addressing violations that occur).

Improving Collaboration on Privacy Risk Management

The third panel of the day considered how privacy can be better protected through the use of risk assessment and management strategies. A number of different types of risks can be identified. The obvious risks are to individuals, but they are not always well placed to manage those risks. Other privacy risks include those faced more broadly by society, which can be damaged by incidents like data breach even where individuals are not directly harmed. But the primary focus of the panel was the risks faced by organisations, both in terms of compliance and reputation.

One of the key ways identified to address such risks is privacy impact assessments (PIAs). A number of authorities have provided guidance on developing PIAs, which assist organisations to engage in a process to think about privacy up front at the design stage. This can help avoid expensive after-the-fact adjustments to a system where needed to address privacy issues. However, it was pointed out that a PIA can be labour intensive and therefore hard to implement consistently across an organisation.

One counterpart to a PIA is a trustmark or “accountability agent” to help promote privacy governance and compliance for private sector organisations. Trustmarks can assist organisations, large and small, to deal with privacy risks, establish and maintain reputations, better understand basic privacy requirements and promote compliance. It was suggested that this type of third-party involvement can be particularly helpful in filling the gap in countries that do not yet have a privacy law or enforcement authority. Trustmarks can also assist regulators in disseminating guidance, and play a role in educating consumers.

Some organisations are building internal technical mechanisms – e.g., accountability decision tools – to help them balance the tensions arising from the need to use information robustly while ensuring that decisions taken are responsible and accountable. An accountability decision model can allow ethical and risk considerations to be taken into account in addition to the requirements of the privacy policies. One regulator pointed out the importance of training for an organisation’s staff, as complaints and incidents are often due to the actions of someone within a firm.

Coping with Technical Complexity

The final panel considered issues related to the privacy dimensions of evolving technologies and applications, which bring considerable complexities along with the many benefits. It was suggested, in fact, that the increases in complexities may be far greater than users think, given that user demands for simplified interfaces carry a hidden cost in terms of vastly greater “back-end” complexities. Another trend is that elements of services that used to operate discretely now form part of broader ecosystems. This may make it more difficult to accurately assess data flows, uses and privacy risks.

There was consensus that ensuring an efficient information exchange between organisations and authorities on the privacy issues associated with these changes was difficult but important. A number of possible ways to address this challenge were identified. For example, beginning the policy dialogue early in the life-cycle of the technology (e.g. the OECD work on RFID) can help ensure that privacy is addressed at the design stage, and not just after a product or service is ready to be rolled-out. Likewise, consideration of the specific technological context – for example, through case studies – can contribute to realistic understandings. It was also highlighted that the dialogue should include end users (not just the technology providers), be international in character, and be an ongoing activity in order to reflect the dynamic character of the subject matter. One suggestion was that dialogue did not always need to have a goal or end result; in some instances, the conversation itself can be the deliverable.

While many discussions between professionals and authorities can and should happen in public – e.g. “Town Hall” meetings, workshops, foresight forums – other conversations may benefit from a more confidential setting (e.g. a dialogue about a future product launch). Indeed, greater attention to finding appropriate mechanisms for permitting private conversations between authorities and professionals may be necessary to ensure that organisations feel comfortable engaging the authorities without risk of alerting competitors or the press about sensitive issues.

Company privacy officers – which enjoy special status under German, French and other national laws – are often very well positioned to facilitate the sort of open, constructive dialogue with authorities to help address privacy issues before they become problems. The increasing complexity of technologies and the applications they support can raise novel questions about how to apply privacy principles and laws, highlighting that the need for open dialogue between professionals and authorities is only likely to increase.