International Chamber of Commerce
The world business organization

Policy statement

Prepared by the ICC Commission on
The Digital Economy

Cross-border law enforcement access to company data – current issues under data protection and privacy law

Document No. 373/507 – (7 February 2012)

Companies processing data in multiple countries face increasing government pressure to comply with law enforcement and other regulatory requests for access to personal data that conflict with data protection and privacy laws in other countries in which they operate. The growing number of such cases is caused in part by the explosive growth in phenomena such the use of multi-locational servers for cloud computing, which provide efficient, lower-cost services for individuals and businesses. Companies take their legal compliance responsibilities very seriously, including those under both law enforcement requirements and data protection and privacy laws. However, compliance with law enforcement requests should not require companies to violate the privacy and data protection laws of other countries, as well as their commitments to individuals, employees, and customers. The following are two examples of such situations which occur increasingly in practice:

Example 1: Company X does business in many countries, including Country A, a country that lacks sufficient legal protections for personal data. It transfers personal data regarding transactions from countries all over the world to its central database located at its headquarters in Country B. Company X has taken the necessary steps so that its data processing activities are valid under the legal requirements of the countries where it does business. These legal requirements include that Company X will only process data for purposes defined at the time of collection; that it will provide a legal basis for onward transfers of the data to third parties; and that it will only transfer the data to third parties if steps are taken to provide adequate protection in the country to which the data are transferred. In addition, the consumer privacy policy of Company X states that it will use personal data only for limited specified purposes and provide adequate protection for onward transfers of personal data.

Law enforcement authorities in Country A approach Company X stating that they have suspicions that certain individuals with which Company X has transacted business may be involved in illegal activities. The individuals are citizens of multiple countries, including those of Country A. These authorities then request Company X to turn over to them all records Company X holds involving transactions with such individuals over the last three years, including those stored at its database in Country B. The request is not based on a judicial order, and does not list any further details beyond the names of the individuals and the timeframe in which the relevant transactions took place. The authorities state that if this request is not complied with, they will initiate criminal proceedings against the management board of Company X's subsidiary in Country A.

Example 2: The same facts as in Example 1, but instead of asking Company X to transfer transaction records to it, the authorities request Company X to monitor all interactions it has with certain individuals whose records are stored in its database on an on-going basis, and to inform the authorities of any transactions these individuals enter into. No judicial order or legal basis are cited as grounds for this request.

While some countries or regions have legal frameworks for reconciling law enforcement requirements with those under data protection and privacy law, many do not, which can create major problems for companies, including the following:

- ***Conflict with privacy and data protection laws*:** In many cases law enforcement requests may conflict with data protection and privacy laws, including those of other countries where the data were originally collected or where they are stored. For example, in the instances described above, the transfer to law enforcement authorities in Country A may be deemed under the data protection law of Country B to be disproportionate and to violate legal requirements regarding international data transfers. The data protection and privacy laws of the countries where the individuals are located may also "attach" to their personal data and continue to apply as these data are transferred internationally, so that such laws may be violated if the data are subsequently disclosed to foreign law enforcement authorities. These conflicts with privacy and data protection law exist in addition to those that may arise between foreign law enforcement requests and other bodies of law, such as laws and regulations aimed at protecting a country's sovereignty (e.g., so-called "blocking statutes"), legal privileges, banking secrecy laws, and laws on trade secrets, which may all apply to personal data.
- ***Violation of commitments to individuals, employees and customers*:** Authorities' requests for disclosure of data of customers, employees or other individuals may also violate commitments made by companies to these persons (for example, in the companies' privacy policies or regulatory commitments vis-à-vis the employees' representatives bodies). This can lead both to legal liability and a loss of reputation.

- ***Risks of political tensions*:** Political tensions between countries may arise when law enforcement authorities in one country request companies to disclose personal data collected or stored in another one, and companies may be caught in the middle.
- ***Impact on business decisions:*** The legal and political risk and uncertainty caused by such conflicts of laws may have a negative impact on companies' decisions to invest in countries that impose them, and thus impede the flow of international commerce.

These sorts of conflicts are an increasing problem given the growth in cross-border data flows, extended use of distributed Internet data processing technologies (such as cloud computing), and the resulting expansion in illegal activity on the Internet. In the long term, these issues can best be resolved through harmonization of international rules on access to data, and by cooperation between governments where rules remain inconsistent (e.g. through treaties, and enhanced judicial and police cooperation). But harmonization will be a long and complex process, and some conflicts between national laws will likely always remain. **Accordingly, ICC urges law enforcement authorities and governments to take the following actions, some of which have already been advocated by ICC in existing policy papers (such as in the ICC Global business recommendations and best practices for lawful intercept requirements of June 2010)[1]:**

- Take into account the possibility that law enforcement requests may violate the data protection or privacy law of other countries.

- Make requests for access to data only in writing and in accordance with written law and/or local regulation, rather than through informal requests. State clearly in any request the specific legal basis for it and the name of the requesting responsible authority.

- Make cross-border requests for data stored in another country through mutual legal assistance treaties and procedures (MLATs) within existing frameworks, ensuring appropriate involvement of authorities in the countr(ies) where data are stored. Improvements should also be made to existing MLATs so that they (1) cover evolving IP-based communications services; (2) deliver requested data in timeframes satisfactory for law enforcement authorities; (3) increase legal certainty for compliance with respective national laws; (4) give companies sufficient information to interact with the MLAT process in an efficient manner; and (5) create a single point of contact with law enforcement authorities in each country.

- Give companies the opportunity to ascertain the legitimacy of the request and inform the authorities (including their own national authorities) about their obligations under data protection and privacy law, when this is required.

- Be as specific and concise as possible about the scope of the request (such as which data the authority is seeking and for which timeframe), and minimize the amount of data requested.

- Avoid developing mechanisms that compel companies to enter into supposedly "voluntary" agreements to deliver up information under threat of significant, penal, financial, or tax sanctions or local business suspension if they do not.

- Allow companies to limit potential liability, for example by anonymizing or shielding personal data of third parties that are not under investigation.

Implementation of these recommendations would allow more efficient compliance with legitimate public and law enforcement requests, better allow companies to cope with conflicting legal obligations, promote compliance with data protection and privacy laws, and strengthen the flow of international commerce by giving companies the increased legal security they need to plan investments.

:-:-:-:-:-:-:-:-:-:

1 The ICC policy statement entitled *'Global business recommendations and best practices for lawful intercept requirements'*, dated June 2010, can be found here: http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373492LawfulInterceptPolicyStatementJune2010final.pdf

The International Chamber of Commerce (ICC)

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the last century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rules-setting, dispute resolution and policy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on vital technical and sectoral subjects. These include financial services, information technologies, telecommunications, marketing ethics, the environment, transportation, competition law and intellectual property, among others.

ICC enjoys a close working relationship with the United Nations and other intergovernmental organizations, including the World Trade Organization, the G20 and the G8.

ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with their members to address the concerns of business in their countries and convey to their governments the business views formulated by ICC.

ICC Commission on the Digital Economy

Business leaders and experts develop and promote the continued and stable growth of the Digital Economy, and further adoption of its underlying ICT foundation, through regulatory advocacy of key business positions and best practices through ICC's Commission on the Digital Economy.

Through its members who are ICT users and providers from both developed and developing countries, ICC is recognized in expert circles as the global consensus voice for private sector expertise on policy matters that drive the Digital Economy. It also provides the ideal platform for developing global voluntary rules and best practices for this area of interest to companies worldwide. Dedicated to the expansion of secure ICT-facilitated trade, ICC champions the liberalization and regulatory harmonization that are required to achieve a free flow of information across all borders.

ICC led and coordinated the input of business around the world to the United Nations World Summit on the Information Society (WSIS), Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda through its initiative, Business Action to Support the Information Society (BASIS http://www.iccwbo.org/basis).

International Chamber of Commerce
The world business organization
Policy and Business Practices
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org