Worldwide usage control of digital data and computer programs

BIC Discussion Paper **November 2012**

Michel Riguidel [1]

1 Telecom ParisTech, France

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction – need for INCO

Background, definition of the topic

With the global development of network activity without borders, digital data and computer programs for users and businesses are increasingly under the management or direct control of third parties, mostly outside the borders of countries of the owner or his responsible: cloud computing, social networks, search engines, mobile applications, micro-blogs, distributed games, messages, etc.

Research challenges involved with the topic that require INCO

Usage control of computer entities (equipment, services, applications, data, and multimedia content) is a fundamental problem in digital security. There is no technical measure to fully resolve this issue, because the volatility of an entity is a consubstantial digital property: one can endlessly create, store, destroy, copy, modify, process and transmit data or a program. There is no technical measure to fully guarantee programs or data security, whose one is either owner or responsible and which are managed and controlled by third parties.

This is the problem of usage control (DRM, software license, distribution of multimedia content) and the problem of cloud computing security, or the issue of right to oblivion for personal data distributed on the net.

- Many personal data are managed by third parties (service providers on the network), created by third parties (mobile operator, bank), stored or handled by search engines, without authors, owners, or those responsible for this data or these programs have a real feedback on these data, or even scrutiny.
- Some personal data are created voluntarily, in a certain context by the people, but then become sensitive and out of their control (photo on mobile phones, personal data on social networks). Modification, annotation or erasure of data is almost impossible due to a massive boom on a content or media lynching. Other personal data are created without the knowledge or consent of people, and out of their control (recording of geo-location, bank records, database created by search engines).
- Most application software is now distributed on the network, with different business models (pay per use, license and subscription) without absolute secure lock.
  In practice, usage control is implemented by some technical measures that have heavy vulnerabilities (DRM, hardware lock, electronic signature, etc.). Its implementation is actually complemented by organizational measures when it is confined to a specific area (eg project management), or legal action when it is confined in a single country (laws on intellectual property or on usage of computer resources).

Objectives of the topic that require INCO

The problem becomes more acute at the international level (cloud computing, DRM, multimedia download, software distribution), because States have not yet harmonized their legislation on counterfeiting, illegal use of content, on the data commodification, on intellectual property of programs and data, on compliance with the private info-sphere, on malevolent usage of data and programs.

- How to make computer usage less opaque: resources used, circulation and storage of data are made more opaque by virtualization. Virtualization brings a de-correlation between the physical and logical resources.
- How to change the relationship to the supplier, which has an increasing responsibility and to which a hard auditable security assurance is assumed. Do we have models to identify trustworthy providers over time?

In addition, threats exploit regulatory vulnerabilities: data governance is an issue of sovereignty. Finally, irreversibility of the access to digital data is a threat: message delivery without post-security from the recipient, proprietary format of clouds, data on social networks without time constraint, etc.

The research objective is to develop a legal and technical framework to provide security, trsut and privacy for data (personal data and software for individuals and/or enterprises) that takes a transnational perspective. This would take into account the set of technical requirements, the new context (cloud computing, social networks) for software editors and service providers to implement such environment.

The expected outcomes of dealing with that topic

An overall framework for sharing, exchanging data and programs would redesign the legal conditions, obligations and constraints of using software and data (multimedia content, etc.) in the new ecosystem: issues of copyrights, privacy questions, peer-to-peer exchanges, etc.

Stakeholders

- Software editors that are designing services, ISPs and Telcos that have access to data. They typically need to protect intellectual property, privacy, reputation and revenues and would need an overall solution.
- National and international legal and technical academics, legislators and regulators.

Benefits and success metrics, and need for INCO

The lack of protection is an obstacle to the adoption, by individuals or companies, of innovative services (public cloud computing for businesses, networked applications for individuals).

Approach

Software editors and software engineering academics are best suited to take initiatives. Then ITU and international software engineering associations could test the deployment of such framework. A multilateral and a continent to continent (America, Africa, Europe, Asia) approach is needed due to the different cultures for properties and privacies.

International cooperation in software security is too dispersed. Software engineering is too focused on formal methods and not on cross-disciplinary questions as security, property, authorship.

Timescales

It is necessary to conduct research at the international level, both technical and legal, to fill this gap, which is an obstacle to the development of digital services:

Research until 2015

Recommendation for Research – R1:
– *security models*

- Security Policy of outsourcing services;
- Model of security, trust and privacy of data or programs controlled by worldwide third parties;
- Design and implementation of security models, trust models, privacy model on services applicable to personal data and behavioural data, recorded unbeknownst to the people.

Recommendation for Research – R2
- *architectures and services*

- Development of technical measures for the right to be forgotten (erase data after a certain period)
- Method and tools for the right to change (deletion, annotation, etc.) personal information.
- Design and deployment model of entrustment, delegation of management by a third party.
- Rules of monitoring or audit of management by a third party.
- Usage control model (a priori, a posteriori)
- Access control model, with information and / or permission of the authors or indirect control
- Security policy of outsourced data management
- Security of public cloud computing

Recommendation for Research – R3
- *legal framework*

- Security of DRM, security model of intellectual property
- Secure communications with scrutiny on the operating post messages.
- Security model in association (information on usage of personal data)

Recommendation for Research – R4
- *ethical, economical dimensions*

- Ethical usage of computing resources, data, programs
- Audit of the usage

Implementation 2015 - 2020

Then the validation of several instantiations of the framework could be tested at the national and continental levels.

About the Author
Michel Riguidel is now Professor Emeritus (since May 2010), and previously the Head of the Department of Computer Science and Networks, at Telecom ParisTech (École Nationale Supérieure des Télécommunications, http://www.telecom-paristech.fr) in Paris, where he lectures in security and advanced networks. His research is oriented towards security of large Information Systems and Networks and architecture of communication systems (Security of the Future Internet, Trust, Privacy and Advanced Networks).
In the European Projects, he was Key Researcher of the Secoqc Project (Development of a Global Network for Secure Communication based on Quantum Cryptography). In the FET of the FP6, he was the Security & Dependability Task Group Leader of the Beyond the Horizon Project. He has contributed to the FP7 CAs of the ThinkTrust, IncoTrust (2008-2010) and BIC (2011-2013).
He has several patents in security (firewall, watermarking and protecting CD ROM, illicit content downloading, security of communication).
In 2013, he is currently working on BIC and on the security of the Future Internet, especially with JiaoTong University (Shanghai) and Huawei.