Joint Research Centre (JRC)
Traceability and Vulnerability Assessment Unit

Towards a better understanding of the impact of emerging ICT on the safety and security of the Citizen
Digital Citizen Security - a programmatic approach

Ioannis Kounelis, Jan Löschner, **Vincent Mahieu**, Sead Muftic[1], Jean-Pierre Nordvik, Pasquale Stirparo

IPSC - Institute for the Protection and Security of the Citizen
Ispra – Italy   *http://ipsc.jrc.ec.europa.eu*

KTH[1] - Royal Institute of Technology
*Stockholm – Sweden*   *http://www.kth.se*

Our Organization

The Mission of the Joint Research Centre is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies.

The Institute for the Protection and Security of the Citizen provides research results and supports EU policy-makers in their effort towards global security and protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

Since 2011 the new Traceability and Vulnerability Assessment Unit is addressing the impact that new information and communication technologies have on the citizen.

The European citizen as an individual is put to the centre of the considerations that will address issues such as the acceptance of new ICT, data protection and privacy concerns, security ethics, citizen profiling and electronic traces.

❖ The Citizen Digital Footprint (CIDIPRINT) action which will develop and assess scenarios associated with information recorded when a citizen interacts in a digital smart environment, in particular with the internet of the future and with intelligent transport systems

❖ The Security Aspects of the Digital Society (SIDSO) action which will detect and anticipate potential societal implications of emerging Information and Communication Technologies

❖ The Surveillance Systems and the Citizen (SURCIT) action which will assess existing and emerging technologies and solutions for surveillance and monitoring

The Policy Context
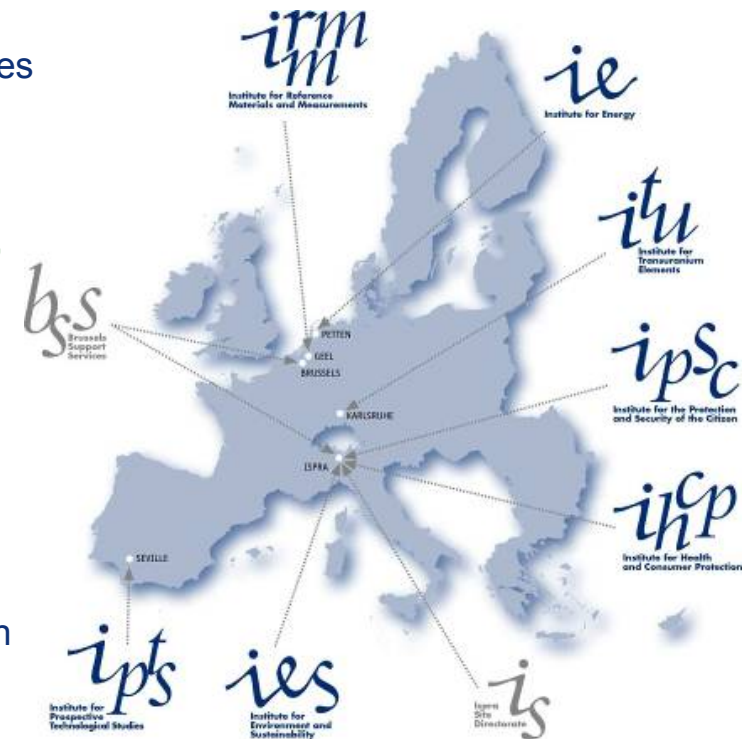
Emerging ICT is changing our society in a revolutionary dimension

The Joint Research Centre (JRC), by assessing the exploitation of digital personal data, responds to some of the key challenges put forward in the Communication from the Commission "Europe 2020" and to one of its flagship initiatives, "A Digital Agenda for Europe".

The issues addressed are namely: Trust and Security, a vibrant digital single market and Intelligent Transport Systems for safer, more secure and more efficient transport and better mobility in Europe

The European Commission is promoting, amongst others, the Stockholm Program for an open and secure Europe serving and protecting the citizens.

The European Commission (EC) formulated as a response to the economic and financial crisis its strategy for smart, sustainable and inclusive growth, in which the "five measurable EU targets for 2020" are defined.

Those targets include amongst technical ones, the social, ethical, institutional and legal implications of research and development of emerging technologies.

The ETICA project states for example: "If societies want to be proactive in addressing technologies possible ethical issues, they need to have some reliable way of identifying these technologies."

The review of the EU Data Protection Directive in these days does not come as a surprise. One of the main policy objectives for the European Commission is to modernize the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalization and the use of new technologies.

JRC — EUROPEAN COMMISSION

iPSc — Institute for the Protection and Security of the Citizen — KTH VETENSKAP OCH KONST

> An interdisciplinary approach, between technology and social sciences

The main objectives of the Traceability and Vulnerability Assessment Unit:

❖ Assess the <u>implication of emerging ICT</u> on the citizen in a structured and substantiated (i.e. scientific) way
❖ Focus on the <u>citizen</u> and his <u>perception</u> using ICT or interacting with the digital world
❖ Broaden a purely technological approach to an interdisciplinary one including <u>societal</u> and <u>legal issues</u>
❖ Develop and assess <u>scenarios</u> associated with information recorded when a citizen interacts intentionally or non intentionally with ICT
❖ Detect, anticipate and prioritize potential <u>society implications</u> of emerging ICT's.

The strategy is based on 3 pillars:

❖ The <u>experience</u> and <u>expertise</u> gained in the past by developing, evaluating, and applying methods for assessing vulnerabilities of complex systems and infrastructures, exposed to technological, manmade (voluntary or not) and natural hazards

❖ Closed links with other <u>Directorates General of the European Commission</u> to facilitate an optimal policy interaction

❖ A strategic partnership with key research partners and an active participation to relevant <u>thematic expert networks</u>

Where are we planning to go ?

Possible Bluetooth threads
    Surveillance: by acquiring specific details about a Bluetooth device to assess possible vulnerable vectors
    Traceability: Sniffing and Eavesdropping. Bluetooth broadcasts traffic wirelessly, therefore is prone to external monitoring of specific frequencies, e.g. eavesdropping of phone calls
    Denial of Service: especially in security applications

Potential NFC (Near Field Communication) threads
    Loss or theft of the mobile device, which will imply for the citizen to lose all at once his personal/private information
    stored on the phone and his credit card,
    Sniffing and Eavesdropping of the radio signal during payments session
    Unwanted and unsolicited payment triggered by a malicious person getting closed to the citizen who is carrying a NFC enable mobile device.

Distributed applications
    Mobile architectures for trust
    User Identification with the use of the Universal Integrated Circuit Cards (UICC)
    User Profiling
    Mobile Ad-Hoc Networks
    Interoperable cross border e-signatures for digital transactions
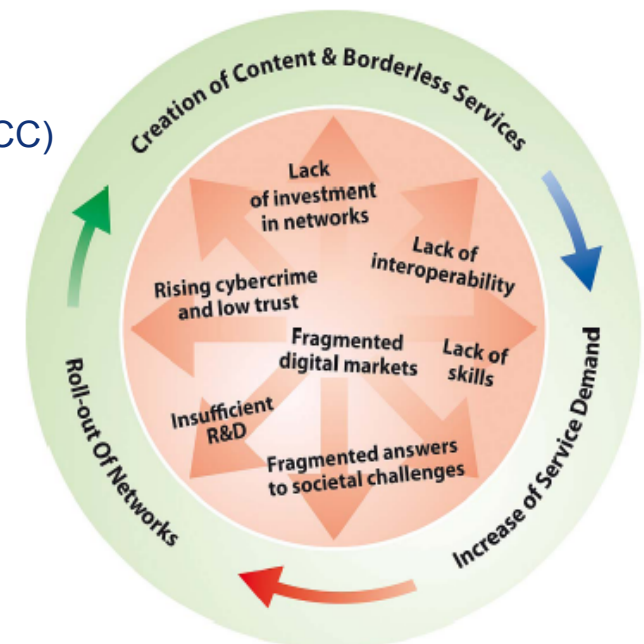
Mobile Cloud Computing
    User Privacy
    Availability
    Resilience
    Limited mobile resources

Mobile Operating Systems
    Digital Forensics

Joint Research Centre (JRC)

Robust science for policy making

J. Löschner, **V. Mahieu**, P. Stirparo, J.-P. Nordvik, I. Kounelis

Citizen Digital Footprint Action

Traceability and Vulnerability Assessment Unit

Institute for the Protection and Security of the Citizen

Web: www.jrc.ec.europa.eu

Contact: vincent.mahieu@jrc.ec.europa.eu

School of Information and Communication

Technology Royal Institute of Technology (KTH)

Sead Muftic

Contact: sead@kth.se