Fundamental Rights Forum
connect.reflect.act

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Working group 25:

The role and responsibility of business in respecting privacy in a context of increased security in Europe: Challenges and promising practices

Background

In the framework of current and future legislation on national security, the private sector is often obliged to retain users' data and provide access upon authorised request. The recent Passenger Name Records (PNR) Directive as well as national laws on access to communications data are just some examples. As a result, private companies have increasingly been faced with situations in which they are expected to comply with conflicting legal obligations.

In policy debates aimed at finding a balance between these contrasting needs, regulators, such as national Data Protection Authorities, or private companies have often endorsed users' rights to data protection and the respect of personal and family life. They have done so by encouraging the use of encrypted communication and by publishing so-called transparency reports on access requests from national intelligence services and/or law enforcement authorities. (See, e.g., https://www.google.com/transparencyreport, https://govtrequests.facebook.com, https://transparency.twitter.com.) Such measures are believed to empower the user, protect proprietary IT systems and maintain the necessary checks in a democratic society.

Another aspect that needs to be discussed is to what extent providers of email services, which are not telecommunication companies, are subject to Member States' telecommunications laws since they provide functionally equivalent services. If this is the case, they too may be subject to the same considerations as telecommunications companies.

Objectives

This workshop sought to explore how the business sector deals with legal obligations in the context of national security. It examined how business balances such obligations with the need to uphold fundamental rights, in particular respect for personal and family life, as well as the right to data protection. Transparency about requests from governments to access personal data is increasingly being raised in ongoing policy debates on national security measures. The panel aimed to discuss practical issues with representatives from the private sector who have recently taken relevant initiatives in this field.

Speakers

- Erich Schweighofer, Professor, University of Vienna, Centre for Computers and Law
- Michal Boni, Member of the European Parliament, former Minister of Administration and Digitization of Poland
- Joseph Cannataci, Professor, UN Special Rapporteur on the Right to privacy
- Gail Kent, Head of Security Policy, Facebook
- Cornelia Kutterer, EU Government Affairs & Digital Policy Director, Microsoft

Main messages

1. 'Let's not reinvent the wheel' – instead, first try to better implement and evaluate existing legal frameworks on data/privacy protection on different levels (international treaties, EU law, soft law).
2. This is a fast-changing environment with many potential risks and opportunities from a fundamental rights point of view. As it takes a long time for new legislation/treaties to be in place, a lot can be more quickly done by way of "pilots", such as codes of conduct and self-regulation, or partial regulation of the field. From these we can learn lessons regarding further adjustments. For example, start regulating medical data online partially, focusing first on e-Health applications, for example.
3. The cooperation of all stakeholders – including international organisations, national governments and parliaments, as well civil society and business – is key for protecting privacy and personal data, and raising citizens'/users' ('data subjects') awareness. Involvement, consultation and transparency in setting new rules are crucial for Europe to safeguard privacy and protect personal data on the one hand, and to allow Europeans to enjoy the advancements of technology on the other. For example, effective medical treatment will be more and more personalised, but vast quantity of personal data will need to be processed to make it effective. Rights to security and privacy do not contradict each other ('security or privacy' is a false alternative). There is a need to carefully examine what limitations to the interrelated rights of privacy, data protection, freedom of expression and security are legitimate, proportionate and needed.

Promising practices

- The PNR Directive, developed by EU institutions and Member States, includes clear rules on the purpose of data collection, transfer and retention, making it a model that can be repeated in other areas.
- The Global Network Initiative is a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics. They spent two years negotiating and creating a collaborative approach to protecting and advancing freedom of expression and privacy in the ICT sector. It was developed in response to governmental pressure on ICT companies

to comply with domestic laws and policies in ways that may conflict with these rights.

Next steps

- IT companies and public authorities need to more effectively raise awareness about privacy and other user rights.
- Users, civil society organisations, and active citizens, supported by public authorities should, in cooperation with business, raise digital citizens'/users' awareness of their rights and obligations online. For example, users should read privacy and user rights carefully, and sometimes pursue strategic litigation if needed.
- All partners (international, national, CSOs, business, active citizens) should discuss what limitations to the interrelated rights of privacy/data protection, freedom of expression and security are legitimate, proportionate and needed. Cooperation of all partners is crucial, and discussions should take the form of common debates rather than separate discussions. This should be followed-up on during the October meeting of oversight authorities organised by the UN Special Rapporteur on the right to privacy.
- EU institutions and Member States, in consultation with civil society and business, need to harmonise EU Member States' legal standards within existing EU/international legal standards/obligations.
- There is a need for global standards. EU institutions and Member States should pursue an EU agreement and other regional agreements to make international negotiations easier and faster (transferability of practices/standards).
- Citizens, consumers, users and business should promote encryption technologies, and bring government to discussions on the mass use of encryption.
- EU Member States should ensure better oversight of surveillance activities. This includes putting in place efficient systemic safeguards (expert bodies) and individual remedies, which would lead to sustainable security; security measures with infringement of fundamental rights are not sustainable.
- Regarding medical data, EU institutions and Member States should map applicable legal standards within the EU. In case of advanced reverse data engineering, it may be possible to extract individual data from the statistical data, which could pose a tremendous threat to fundamental rights.
- EU agencies, supported by EU institutions (including LIBE), should foster cooperation between ENISA, FRA, Europol and other EU agencies in that area.
- Member States, assisted by EU institutions if needed, should provide clear definitions of key terms such as 'terrorism', 'national security', etc., to avoid misuse by law enforcement/internal security agencies.
- Standards bodies should ensure coherence. Specifically, the International Organization for Standardization (ISO) and European (EN) standards should be cross-checked against each other and other existing norms (as they may be incoherent).