SSH IN ICT USING THE EXAMPLE OF TRUESSEC.EU

Martin Griesbacher / Elisabeth Staudegger / Harald Stelzer

MA., University of Graz, Department of Sociology
Universitätsstraße 15/G3, 8010 Graz, AT
m.griesbacher@uni-graz.at; http://sociology.at/mag

Univ.-Prof., Universität Graz, Institut für Rechtswissenschaftliche Grundlagen, Fachbereich Recht und IT
Universitätsstraße 15, 8010, Graz, AT
elisabeth.staudegger@uni-graz.at; http://rewi-grundlagen.uni-graz.at/de/institut/recht-und-it/team/

Univ.-Prof., Universität Graz, Institut für Philosophie, Arbeitsbereich Politische Philosophie
Heinrichstraße 26, 8010, Graz, AT
Harald.stelzer@uni-graz.at; https://philosophie-gewi.uni-graz.at/de/politische-philosophie/

Keywords: ***ICT products and services, SSH, trust, certification, labelling***

Abstract: *This article deals with the implementation of Social Sciences and Humanities (SSH) in ICT-products. It explains the arising challenges through the Coordination and Support Action TRUESSEC.EU which receives funding from the European Commission. As the European Union advances the Digital Single Market, users are concerned about the trustworthiness of ICT-products and services. Certification can be vital in restoring transparency and trust. TRUESSEC.EU aims to build an enduring StakeHolder' Online Platform (SHOP) and to work out REcommendations for Trust Enhancing Labels (RETEL), both based on SUPPorting Analyzing studies with a strong focus on SSH (SUPPA).*

1. Starting position

The Digital Single Market (DSM) strategy is one of the explicit priorities of the European Union.[1] It is well known that confidence in the digital environment is an indispensable prerequisite in the pursuit of this strategy,[2] only 22% of Europeans have full trust in diverse company offerings, such as search engines, social networking sites and e-mail services. Moreover, 72% of internet users are concerned about being asked to disclose too much personal data online.[3] The Special Eurobarometer 431 (Data Protection) summarizes the report's findings: «The level of trust in online companies remains noticeably low.»[4]

In practice, it is difficult for consumers – individuals as well as organizations – to appraise the trustworthiness of the services they use. The key attributes of trustworthiness, such as security, privacy, robustness, etc., are «credence qualities» which cannot be easily evaluated. Nonetheless, they represent the fundamental aspects of internet-based goods.

The increasing adoption of highly complex and interdependent cyber-physical systems across a wide range of important everyday domains, such as healthcare, retail, connected vehicles, SCADA (supervisory control and data acquisition), domestic IoT (Internet of Things; e.g. smart home products) and trans-national in-

1 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final.

2 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final/2, see 2.1.3. Building digital confidence and 2.3. Trust and security.

3 For further details see Special Eurobarometer 423 (Cyber security), http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf (all Websites accessed on 24 January 2017), Special Eurobarometer 431 (Data protection), http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf and Special Eurobarometer 432 (Europeans' attitudes towards security), http://ec.europa.eu/public_opinion/archives/ebs/ebs_432_en.pdf.

4 Special Eurobarometer 431 (Data protection) p. 115, http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.

frastructures, such as cloud platforms, complicate the situation even more. These systems increasingly use a multitude of components manufactured by third parties in complex supply chains. Most of these products stem from outside the European Union. This bypasses the jurisdiction of European regulation, aggravating the opacity issue.

Therefore, the DSM is calling for reinforcement of trust and security in digital services and in the handling of personal data. Subsequently, the European Commission calls for proposals about the strategies for attaining this objective.[5]

We consider increased transparency as the only solution. Assurance and certification can achieve this urgently needed transparency, as they provide users with a tool to ascertain the trustworthiness of a digital product without having expert knowledge.

Much activity is under way in this regard in the fields of policy (e.g. Cybersecurity Strategy, DSM Strategy), research and innovation (e.g. H2020 Secure Societies, call topic Digital Security: Cybersecurity, Privacy and Trust) and implementation (e.g. legal instruments: ePrivacy Directive, Network and Information Security Directive, General Data Protection Regulation, practices like privacy labels and seals at Member State levels). In fact, at the moment there are many seals certifying different properties and qualities. Nevertheless, the current studies indicate that they seem to lack efficiency. What, in our view, is still missing is a serious basis of certification with well-defined and generally accepted properties. Furthermore, there is still a lack of measurable criteria for verifying whether the requirements are met in a certain case.[6]

TRUESSEC.EU[7] addresses this challenge from a multidisciplinary perspective, with a strong focus on SSH aspects which support the more technically oriented RIAs (Research & Innovation Actions) and IAs (Innovation Actions) of the same call. It will explore, analyze and share information on the needs for online certification and assurance, behaviors and practices of citizens, industry and businesses in the context of a rapidly evolving internet eco-system. Going beyond the current state of the art, it will assess and disseminate the best emerging practices from consumers and industry to ensure a more resilient and trustworthy European digital market, and will provide an online platform to support this. This work will be undertaken in the context of the relevant European security and privacy regulations.

The project ultimately aims to strengthen the European DSM by facilitating secure, lawful and trustworthy ICT services and products through the improvement of trust-enhancing labels and certifications. European ICT-based products and services can thus become the most trusted in the world, especially in new markets.

2. The Consortium

TRUESSEC.EU is a Coordination and Support Action (CSA) on certification and labelling of trustworthiness properties from a multidisciplinary Social Sciences and Humanities (SSH) and Information and Communication Technology (ICT) perspective with a special emphasis on human rights and European values. The CSA

5 See DS-01-2016 – Assurance and Certification for Trustworthy and Secure ICT systems, services and components, http://cordis.europa.eu/programme/rcn/700809_en.html.

6 See Regulation (EU) 2016/679 (General Data Protection Regulation; GDPR), Official Journal L 119 , 4 May 2016, pp. 1–88, Recital 166: «In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level […]»

7 Concerning TRUESSEC.EU, this article is based on the full text of the proposal written by the teams of all partners (for some further details, see: http://cordis.europa.eu/project/rcn/207202_en.html). We are thankful to all staff members who provided expertise that greatly assisted the research, although they may not agree with all of the details provided in this paper. We are also grateful to *Claire Diot-Lefebvre* who moderated the proposal and *Paul Galvas* for his valuable comments and suggestions on this article. The authors are also grateful to *Aiste Mickonyte*, LL.M., for her reading of the paper and her linguistic suggestions.

builds upon existing activities, bringing together an inter-disciplinary community of stakeholders, encompassing technology providers, public bodies, consumers and concerned citizens from the private, public, research and third sectors across Europe facing the common challenge of the assurance and certification of emerging internet-based technologies in their respective domains.

The coordinator of the project is the Digital Catapult Ltd. (UK). Further participants are the Knowledge Transfer Network Limited (UK), the APWG European Foundation (Spain), and the Asociación de Usarios de Internet (Spain). These members of the consortium (DIGICAT, KTN, APWG and AUI) are partners who embody the stakeholder networks themselves.

The academic sector is represented by the Ingeniería de Sistemas Telemáticos (DIT) of the Universidad Politécnica de Madrid (Spain), the Institute of Philosophy, the Institute of Sociology, and the Institute of the Foundations of Law, section Law and ICT, of the University of Graz (Austria), and the CERAPS at the Faculty of Law of the Université de Lille II – Droit et Santé (France).

The TRUESSEC.EU community will combine private, corporate and institutional actors interested in strengthening consumer trust and fundamental rights in the digital sphere. The community will leverage the already existing networks embodied by four of the project partners themselves, conferring a relevant role to this cluster's projects. The development of the TRUESSEC.EU community and online platform will therefore enable us to work out broadly recognized recommendations for trust labels and thus contribute to the basic prerequisites for a more secure and safe cyberspace in which European values and fundamental rights are implemented.

3. Three Pillars: SHOP, SUPPA and RETEL

The main objective of the TRUESSEC.EU project is to foster the emergence of trust and confidence in new and emerging ICT products and services throughout Europe. This project seeks, in particular, to encourage the adoption of appropriate assurance and certification processes that take into account multidisciplinary (SSH and ICT) aspects, having due regard to the protection of human rights. It is based on three strategic key pillars:

- **SHOP** is the acronym of a **S**take**H**olders» **O**nline **P**latform in which associated cluster projects and stakeholders from the industry, academia, governments and civil society will be invited to participate. It will serve as a platform for the community to put forward and debate proposals and solutions around trust-enhancing labels and other certification and trust mechanisms. It will also be a channel for attracting direct inputs from stakeholders, presenting the outcomes of the project to them, testing its recommendations with the community, and receiving feedback from them. So SHOP will be the interfacing point between TRUESSEC.EU and associated projects within the same call as well as the community of practice at large. Moreover, the SHOP-platform will be used as a repository for material collected and generated during the studies.
- **SUPPA, SUPP**orting **A**nalysis, frames a series of studies from multidisciplinary perspectives on issues of trustworthiness certification and assurance. This is where the SSH-expertise comes in. TRUESSEC.EU will identify existing stakeholders, initiatives and labels, and analyze their legal, ethical, socio-cultural, business and technological aspects, as well as their impact on the development and use of trustworthy internet-based technologies. This analysis – combined with a review of scientific literature, policy and legal documents – will be carried out from the scholarly perspectives of sociology, culture, law, ethics, political philosophy, and economics/business management. Based on the results of individual studies, a framework outlining fundamental rights as well as relevant legal provisions will be established. On the basis of the theoretical reference framework, a Criteria Catalogue will be elaborated, defining a set of high-level principles relevant for assurance and certification of trustworthiness in ICT systems, services and components. These principles will be operationalized through guidelines for optimal criteria, which represent technical requirements that are closer to technology and easier to

understand for technology developers. Mapping, creating and selecting criteria and indicators found in theory and in practice will assist the improvement towards a harmonized European approach.

– **RETEL** refers to a set of **R**ecommendations on **E**uropean **T**rust-**E**nhancing **L**abels dealing with the methodological aspects of certification and assurance. After completing the theoretical analysis and individual studies in SUPPA, and following the debates with stakeholders through the SHOP-platform, TRUESSEC.EU will issue a set of recommendations for trustworthiness labels. For this purpose, a set of criteria and accompanying measures for European Trust-Enhancing Labels will be devised and discussed through the SHOP, enabling the community to contribute to the enhancement of these recommendations. Rather than defining a «yet another» label, TRUESSEC.EU will provide a set of label-neutral results that can be taken advantage of by any label whatsoever wishing to adopt them. These recommendations include a multidisciplinary Criteria Catalogue which can be used by labels, and which considers technological, sociological, cultural, legal, political, ethical, human rights and business aspects; methodological recommendations for assurance and certification for a European trust-enhancing label for ICT systems, services and components; and recommendations for accompanying standardization and regulatory measures for policymakers.

In order to combine the TRUESSEC.EU research-supporting action and the stimulation of the community coordination, the project approach is based on the integration of these three types of activities, whereby each of them is continuously interrelated with the other ones. The tasks are structured into eight work packages: WP 1 carries out the overall management; WP 2 develops engagement with stakeholders (SHOP); WPs 3, 4, 5 and 6 (SUPPA) are devoted to studies of the interdisciplinary sociological, cultural, legal, ethical, business and technological factors; WP 7 is concerned with issuing the recommendations for a trust-enhancing label (RETEL); and WP 8 is concerned with dissemination, exploitation, and communication.

4. SSH in Focus: Legal, Ethical and Sociological Perspectives on Cybersecurity

Seeking to provide an exemplary insight into the multidisciplinary studies conducted to support TRUESSEC.EU, the present section highlights the legal, ethical and sociological perspectives.

A trust-enhancing label is in any case capable of confirming that a particular certified product complies with the applicable legal requirements. However, due to the enormous technological progress in the field of ICT, the relevant provisions change in rapid succession. Even for lawyers it is immensely difficult to know and understand all the applicable law. Therefore, we aim to elaborate an in-depth analysis of the existing legal framework as well as a comprehensive understanding of the legal factors related to ICT security and privacy features. A legal study on ICT-law must first consider the EU legal framework for ICT products and services. Special emphasis should be placed on privacy issues, in particular, on the General Data Protection Regulation. Further legal rules (e.g. concerning E-Commerce[8] or Copyright,[9] not to mention the challenges arising from data aggregation[10] or data ownership) must also be taken into account. Moreover, the European Commission announced[11] at least 16 measures to boost the DSM,[12] amongst them a number of proposals for digital con-

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market («Directive on electronic commerce»), Official Journal L 178, 17 July 2000, pp. 1–16.

[9] For example, see: Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22 June 2001, pp. 10–19.

[10] See: BSI 2015. PAS 1192-5:2015 Specification for security-minded building information modelling, digital built environments and smart asset management. May 2015.

[11] For further announcements concerning European priorities, see: https://ec.europa.eu/priorities/announcements_en.

[12] For an overview, see: http://europa.eu/rapid/press-release_IP-15-6321_en.htm, http://europa.eu/rapid/press-release_STATEMENT-16-181_en.htm, and http://europa.eu/rapid/press-release_MEMO-16-1896_en.htm.

tract rules[13] and a modern copyright.[14] The further discussion and development of these proposals has to be monitored attentively. There is no doubt that the findings of this discussion will influence the understanding of ICT-law in a general sense. However, with regard to TRUESSEC.EU, more particularly, this legal knowledge is an essential component in the process of contributing to the identification and specification of criteria for a certification mechanism, as referred to in Article 42 GDPR, for instance.

In the field of digital security, new services and technologies raise a host of ethical concerns regarding the protection of citizens» fundamental rights and respect for European values (in particular, peace, democracy, human rights, rule of law, equality, and tolerance). Citizens need to be able to use the internet freely and efficiently, and to do it safely. This includes the protection of their privacy. In order to achieve this, the implemented solutions have to be transparent, time efficient, and understandable for users. Citizens can be expected to trust new digital technologies only if they have a reason to believe that their rights will be protected and their shared values respected. A non-exhaustive list of factors that may give the users grounds to feel this way includes legitimacy, acceptability, credibility, transparency, accountability as well as the citizens» ability to control their own personal information. Clearly, the need for online safety provides the normative basis for cyber-security technology. However, privacy concerns may set limits to its use. As in other areas, we have to deal with conflicts of values in this regard. This balance between information sharing and privacy protection is undeniably necessary in order to serve the safety interests of citizens in the best possible way. Furthermore, issues of procedural and substantive justice arise, especially concerning the balancing of the needs and interests of providers, users and other stakeholders. Emphasis should be placed on the special needs of user groups in different sectors of the society, as well as on those groups whose interests are often marginalized in today's digital community. These issues highlight the importance of normative aspects in the Recommendations on European Trust-Enhancing Labels (RETEL), especially when dealing with the development of a multidisciplinary criteria catalogue for labels and certifications, and the regulatory aspects aimed at fostering their adoption.

The sociological perspective uses the key concepts of trust, acceptance, perceived risks and threats in order to address the issue of cybersecurity. The central assumption is that a threat to (the perception of) cybersecurity are not only explicitly «cybercrime»-labelled actions or events, such as cyber-trespassing, cyber-deception or theft, cyber-pornography and cyberpiracy[15] but also «lawful» actors from areas of economy, industry, politics and even official crime-fighting agencies. This involves the handling of private data by ICT service providers and also governmental surveillance activities which are aimed at capturing cybercrime offenders but can increase the feeling of insecurity in cyberspace. Therefore, matters relating to cybersecurity include not only a question of increased technological security and effective battling of crime but also the perceptions of diverse activities and events related to ICT products and services.

As far as the chosen methodological approach is concerned, survey data and discourse analysis are of special importance for the study of public opinions in Europe with regard to the sociological cybersecurity issues.

---

13 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content,COM(2015) 634 final – 2015/0287 (COD).

14 On 14 September 2016, the EC set out 5 documents: 1) Communication – Promoting a fair, efficient and competitive European copyright-based economy in the Digital Single Market; 2) Regulation laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes; 3) Directive on copyright in the Digital Single Market; 4) Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled and 5) Directive on certain permitted uses of works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society.

15 See: David Wall, Cybercrimes and the Internet, in: David Wall (ed.), Crime and the Internet, Routledge, London/New York 2002, pp. 1–17.

They help to bring in empirically grounded insights and conclusions for improving cybersecurity. The empirical studies encompass two tasks: (1) Collecting and evaluating the existing European and national surveys (e.g. Eurobarometer, ESP, ISSP, Cybercrime reports); and (2) Mapping out the exemplary public discourses at European and national level *via* discourse analysis. Overall, the sociological perspective is particularly helpful in understanding the sociocultural differences (e.g. perception of differences of cybersecurity issues across the EU) and raising awareness about the ambivalent reactions to and effects of ICT products and services on society.

5. Conclusions

At present, ICT products and services are widely used across the world. Nevertheless, many Europeans are concerned about security and privacy issues relating to this usage. Since most of the suppliers stem from the US, the majority of these products do not meet the basic European requirements and expectations. Successful implementation of legal, ethical and sociological prerequisites in ICT products, incorporating SSH in ICT, could ensure not only trustworthiness but an even greater market of high quality products.

We are confident that the Recommendations for trust labels and the regulatory measures, along with the development of the TRUESSEC.EU community and the online platform, will pave the way for a more secure and safe cyberspace. This cyberspace will represent an area in which European values and fundamental rights are protected, consumers can have an easy-to-understand tool for verifying existing and emerging products and services, citizens can exert control over their data, and the technology providers and users find a reliable, accountable environment for their activities.