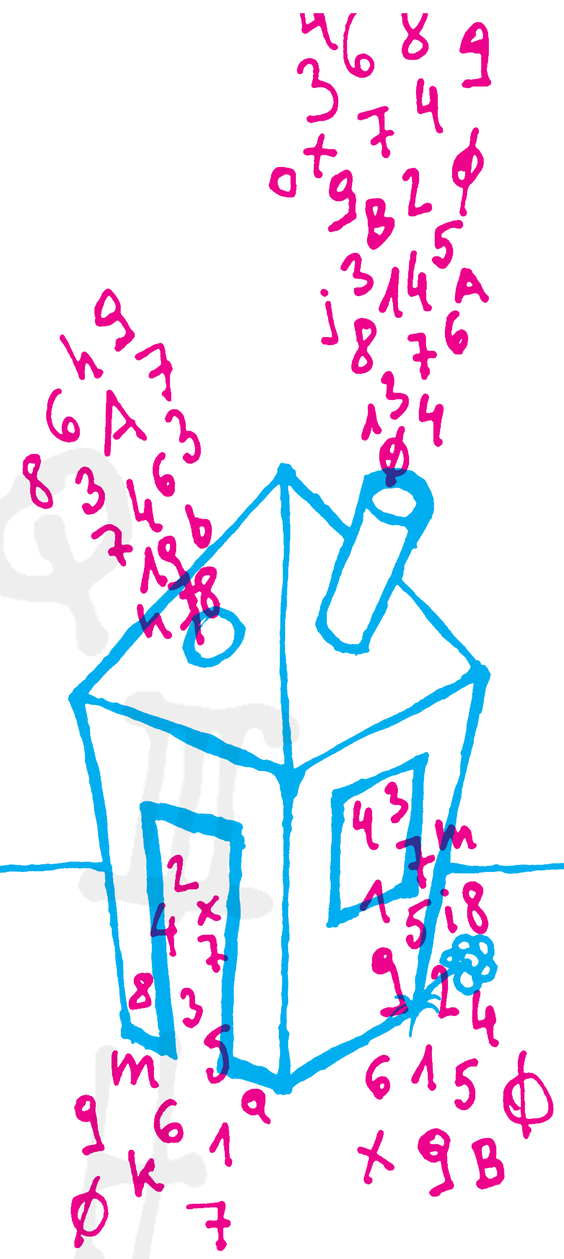
The Need for a Digital Domestic Right



Abstract

The borders between "real" physical world and Cyberspace are blurring. In the light of constantly increasing data power in public and private hand the right to respect for privacy needs specific attention. A renewed and extended definition of privacy is indicated. In the present poster we devise the need for a *digital domestic right*, relating it to the legal concept of the sanctity of the home.

Categories and Subject Descriptors

K.4.0; K.4.1; K.5.0 [Computers and Society]: General, Public Policy Issues, Privacy, Regulation; K.5.1; K.5.2 [Legal Aspects of Computing]: General, Governmental Issues – *Regulation*.

General Terms

Security, Human Factors, Legal Aspects.

Keywords

Territoriality; Human Rights and Fundamental Freedoms; Privacy; Digital Domestic Right.

If you are interested in participating in the "European Citizens Initiative" or in contributing to the organizing of the initiative please do not hesitate to contact us: privacyinitiative@ocg.at

Gerald Futschek
Vienna University of Technology / Austrian Computer Society (OCG)
Favoritenstraße 9-11, 1040 Vienna, Austria +43 (1) 58801 18844
futschek@ifs.tuwien.ac.at

Wolfram Proksch
PFR Attorneys at Law / Austrian Computer Society (OCG)
Nibelungengasse 11/4, 1010 Vienna, Austria +43 (1) 877 0454
proksch@pfr.at

Alexander Prosser
Vienna University of Economics and Business / Austrian Computer Society (OCG)
Nordbergstraße 15, Office A 315, 1090 Vienna, Austria +43 (1) 31336 5630
alexander.prosser@wu-wien.ac.at

Erich Schweighofer
University of Vienna / Austrian Computer Society (OCG)
Schottenbastei 10-16/2/5, 1010 Vienna, Austria +43 (1) 4277 35305
erich.schweighofer@univie.ac.at

Hannes Werthner
Vienna University of Technology / Austrian Computer Society (OCG)
Favoritenstr. 9-11, 1040 Vienna, Austria + 43 (1) 58801 18801
werthner@ec.tuwien.ac.at

1. Introduction

More and more aspects of our life "move" to the Web; the Internet / Web - as the underlying information infrastructure - is increasingly becoming a mirror of the "real" physical world. And it is obviously transforming this world, where it is hard to distinguish between the physical and the virtual. With developments such as the semantic web (moving from the syntax to the concept level) information can be automatically processed and approaches such as web analytics enable statistical / logical inference of new knowledge. Information is becoming transparent. This raises severe challenges for privacy, and it can be foreseen, despite the currently rather careless behavior of (some) users, that this will become a central issue in our societies, also with respect to human rights. In this context we propose the concept of a digital domestic right, relating it to the legal concept of a domestic right.

2. The Legal Concept

In the public international law system of *Westphalian Realism* states are understood as territorially sovereign. States still have the highest authority and powers within their territory.[1] Territorial sovereignty is a commonly accepted and successful principle of peace. The Internet and its virtual spaces - the Cyberspace - are extra-territorial, only virtually territorial. As a result, we are moving to a new world order of global governance with governmental networks and a disaggregated sovereignty.[2] The growing importance of networks of business and civil society should also not be forgotten.

At the early stages the Cyberspace seemed to be uncontrollable. As Johnson/Post stated in 1996, *Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.*[3]

However, after a short time of reflection the States were back and have set standards for online behavior, i.e. legally significant phenomena on the Internet. A borderless world seems now much of a dream that will never happen.[4] Nevertheless, states still seem to be afraid of losing control within "their" territory and with respect to "their" citizens and are strongly considering stricter rules.

Recent measures for the fight against terrorism and organized crime do stipulate serious interference with common human rights - particularly in form of monitoring and interception of all citizens of the Union. In such a way, the directive on data retention 2006/24/EC obliges TELCO-providers to store an abundance of communication data (Internet, telephony) for at least six months. The principle of protection of privacy is turned in the opposite: Everyone is now from the beginning under suspicion. Prevention and sanction are blended. Dangers of abuse or misapplication of stored data are substantially increased. With regard to the access of the national authorities to this data, the directive grants an indefinite discretionary power to the member states in the area of legislation and the adherence to the fundamental freedoms. The principle of proportionality of interventions by a public authority with the exercise of the human rights and fundamental freedoms is not ensured.

In this context it must not be forgotten, that Human Rights and Fundamental Freedoms are central components of the European society. The Treaty of Lisbon authorizes the institutions of the European Union to the improvement of fundamental right protection in Europe.

Article 8(1) of the European Convention on Human Rights defines that "[e]veryone has the right to respect for his private and family life, his home and his correspondence". Paragraph (2) lists a number of, rather broadly, defined cases, where this right may be violated, for instance "in the interests of national security" or "the economic well-being of the country". European case law on this matter, however, seems to have set the boundaries of such intrusion rather narrowly.[5] The domestic right can be considered a "standard feature" in striving for citizen rights throughout the centuries from England (Petition of Rights 1627), via the French constitution of 1795[6] to the various constitutions drafted in the aftermath of the revolution of 1848. The main focus of these regulations seems to have been on the *physical* domicile, only some also included private correspondence.[7] Of late, there seems to be a tendency to generally argue privacy in the digital media by reference to the secrecy of (originally paper) correspondence.[8]

This extension by analogy of the conventional domestic right and secrecy of correspondence, however, will most certainly meet its limitations when "correspondence", even though stretched to the logical limits of the concept, may not be enough to ensure an adequate – and predictable – level of protection. Could, for example, position data of mobile phone customers be considered "correspondence" and hence afford the protection of Art 8 ECHR?

In the light of constantly increasing data power in public and private hands the right to respect for privacy needs specific attention. Erosion or cuttings of this right must be rejected roundly. A renewed and extended definition of privacy is hence indicated – the *digital domestic right*.

The German Federal Constitutional Court has shed some light on this question in its ruling of 27 February 2008[9]. A new fundamental right to the integrity and confidentiality of information technology systems was created. This right must be seen in the context of constraints to on-line investigation methods by the police, but it contains many elements of the proposed right to a digital domestic right.

3. Dimensions

The task, however, is complex and the data to be protected varies due to technological evolution and new services introduced almost every day. This contribution does not profess to define such a digital domestic right, it proposes possible dimensions of such a definition:

- The lieu of data storage should be extended beyond the citizen's premises to other "locations", e.g. the personal laptop or mobile phone, on a server, in network components used en-route, on the body [sensors]). The possible "locations" have to be considered in more detail; open questions are e.g., e-mail account, facebook account, roaming data).
- The lieu of data storage should be protected against interference from Government agencies (typical content of a domestic right). States have a particular obligation to protect the digital domestic right by punishing illegal acts but also providing a supportive environment for a high level of data security. Citizens have to comply with standards of data security.
- Providers and operators (social networks, server farms etc.) have a special obligation to respect the digital domestic right. Use of data has to be transparent and in compliance with contractual arrangements.
- Communication data is protected by the right to secrecy of telecommunications.
- Interference to the digital domestic right is subject to reasons and a judicial authorization.

Independent of these "content" related issues, the proposed digital domestic right is predominantly a political issue. As such the Austrian Computer Society OCG (the authors) is evaluating the possibility of starting a European Citizens' Initiative, which is introduced by the Lisbon Treaty as a new form of public participation in European Union policy shaping. It enables one million citizens who are nationals of a significant number of Member States to call directly on the European Commission to bring forward an initiative of interest to them in an area of EU competence.

[1] Permanent Court of International Justice (PCIJ), Lotus case, 1925; UN Charter, Art 2;„All law is prima facie territorial." (US Supreme Court, American Banana Co. v. United Fruit Co.)

[2] Slaughter, A.-M. 2004. A New World Order. Princeton University Press, Princeton.

[3] Johnson, D.R./Post, D.G. 1996. Law And Borders: The Rise of Law in Cyberspace. 48 Stanford Law Review 1367.

[4] Goldsmith, J./Wu, T. 2006. Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.

[5] Cf. for instance EHRR 493/29(1999), "Smith and Grady vs. U.K.", EHRR 524/1(1975), „Golder vs. U.K.", or EHRR 479/33(2001), "Coster v United Kingdom" or EHRR 0562/04(2004), "S and Marper vs. U.K.", whereby the two latter concern data retention and/or collection cases (S. and Marper vs. U.K. ruled "blanket" DNA collection without concrete suspicion unlawful in the U.K.).

[6] Art 359: "La maison de chaque citoyen est un asile inviolable. […] Aucune visite domicilaire ne peut avoir lieu qu'en virtue d'une loi, […]".

[7] Cf. for instance the Kremsier draft of the Austrian Empire which already also encompassed the privacy of correspondence and required that "[…] die Beschlagnahme von Briefen nur auf Grund eines richterlichen Befehls und nach den Bestimmungen des Gesetzes […]." (Art 8).

[8] The German Federal Constitutional Court, when ruling the German implementation of the EU Data Retention Directive 2006/24/EC as unconstitutional and ordered the stored data to be deleted, also used Art 8(1) ECHR in their argument prominently (private correspondence).

[9] Federal Constitutional Court (BVerfG) 1 BvR 370/07 of 27 February 2008.