Designing freedom? Bringing fundamental rights and freedoms into electricity grids and disaster management through ICTs.

We build liberty...by setting society upon a certain constitution...an architecture...that structures and constrains social and legal power, to the end of protecting fundamental values - principles and ideals that reach beyond the compromises of ordinary politics, Lawrence Lessig (2006)

This application aims to develop research project(s) that will investigate the question of *what happens to fundamental rights and freedoms (such as privacy and dignity) as these become matters of engineering and design to be built into emerging ICT infrastructures*. The project will engage with and study such processes in two domains: (1) smart electricity meters and so-called "smart grids" seen as central to on going transitions towards renewable energies, and (2) ICTs for use in disaster management (ie. search and rescue, "triage"). The research question will be discussed and developed into research proposals in interdisciplinary groups including practitioners from philosophy, social science, law, engineering, software design, as well as representatives of different professions using and operating the ICT systems.

The project addresses the concerns of the SAMKUL program by focusing on rights and freedoms as main legal-political-cultural preconditions of democratic societies, and the ways in which these preconditions are being re-configured and re-constituted in digital technological systems. Such re-configurations are already under way through so-called privacy and data protection by design, through new approaches to risk management, and through the use of ICTs in new environments of energy and disaster management. In these ways the project will specifically addresses the environments of Nature and Technology, and to some extent also Economy[1], as identified in the SAMKUL programme. If funded, we shall arrange 3 workshops with practitioners from the humanities, social science, law, engineering, software development (privacy and data protection by default and design), as well as other practitioners from the relevant fields. The project will run over a period of 2 years. The outcomes will mainly take the shape of research applications to EU (Horizon 2020, Social Sciences and Humanities, Security programme, etc.), and to the Norwegian Research Council (SAMKUL, Security programme, possibly the ICT programme), and possibly also to other European research funding agencies (UK, Netherlands, Belgium). Based on the workshops we will also produce a report for use by the SAMKUL programme and the Norwegian Research Council.

We will make the argument that the developments underpinning the proposal require urgent attention to the situation of fundamental rights in such ICTs-intensive areas as energy and (natural) disaster management. For the Norwegian Research Council and the SAMKUL programme, the results produced will provide inputs, and a broadened knowledge base, for approaching large programmes such as ICTs, energy and security (including risk management as increasingly applied in a number of fields). This requires careful scrutiny also from the social and human sciences, since law is no longer capable of tackling the questions alone, but is itself becoming transformed by

---

[1] Economy is directly dealt with in the case of smart meters, where significant privacy challenges come from economic-regulatory regimes such as demand-side management; indirectly through the ways in which economic thinking increasingly enter into the institutional preconditions in these areas.

developments, in most cases towards more interdisciplinary approaches (including for instance risk assessors, social scientists, engineers and software developers). In the following we shall describe in greater detail the societal and technological developments underpinning the project, and our approach to investigating them.

Digital technologies are increasingly built into infrastructures and environments and relied upon for a number of critical societal functions. This is true also for our physical environments through technologies such as ambient intelligence, sensors in the environments and on the human body, the internet of things, ubiquitous computing, autonomic robotics, smart energy grids and pervasive surveillance systems. All these developments hold out promises to bring ever-more aspects of physical and social worlds together through digital networks and applications. As a consequence, also law is increasingly expected to become responsive to the needs of technology developers and innovators, policy makers and users. If this is to be possible, it is presumed that even fundamental rights and freedoms must be hardcoded and designed into information structures and communication platforms relied upon for critical functions, such as energy provision or search and rescue operations.

Such developments can be observed in various sites: in the judicial domain the German *Bundesverfassungsgericht* has formulated a new "fundamental right in the confidentiality and integrity of information technology systems" in response to practices of hidden online searches on people's computers by public authorities (Bundesverfassungsgericht, 2008); courts have for decades acquired experience with cases about the design of safety and security regulations into technologies, so called "safety by design" (Gambatese and Hinze, 1999), and these practices are now being transferred into new and emerging practices that join law and engineering in efforts towards "privacy and data protection by design". In January 2012 the European Commission published its proposed reform for a so-called general data protection Regulation (GDPR), meant to replace the existing data protection Directive stemming from 1995. This regulation introduces the notion of "data protection by design" (DPbD) for technologies that will process the personal data of people. This notion is new in the legislative universe and the Regulation does not provide many further details about how it is to be applied. It can nevertheless be situated within the larger international field of 'privacy by design' (PbD) and 'privacy enhancing technologies' (PETs), which progressively developed from the 1995 onwards (Hes and Borking, 1995), (Cavoukian and others, 2009). It bears a close relation to 'law as code' (Lessig, 2006) in the US, and more recently at this side of the Atlantic, concepts like 'techno-regulation' (Leenes, 2010) and 'legal protection by design' (Hildebrandt, 2011). Finally, also in the civic domains citizens are asserting their rights in new ways. Tech-savvy citizens are programming the privacy values that they perceive to be at risk directly into digital technologies within collaborative online or offline communities. They also increasingly act in collaboration with jurists and software developers, and challenge large corporations and states with encroachments on their fundamental freedoms before the courts.

On the one hand, and especially following the Snowden revelations, it seems logical and necessary that law, and initiatives to protect and preserve fundamental rights and freedoms, move into the ubiquitous ICT structures that increasingly surround our living, working and natural environments. It seems prudent and precautious to anticipate critical events, developments and actions in these domains. On the other

hand, the same developments pose severe questions, not the least about the nature of law and technology. Traditionally these have belonged within (relatively) separate spheres, with their own way of being and working. What can already be observed is that both are being transformed in the process: ICT systems that are sensitive to rights and freedoms will be decisively different from those that are not; law on it's side will increasingly have to rely upon interdisciplinary collaborations (ie. risk assessors, engineers), and may be pushed towards more anticipatory modes of judging, which is at least partially alien to law. Finally, it seems clear that the described developments constitute a specifically European approach, as such worthy of study and exploration as specifically "European experiments" (Nordmann 2009).

The research question will be investigated in ways that are both empirical and conceptual, through interdisciplinary exchanges between scholars in the humanitites, social sciences and law, with engineers, software developers and the organisations, operators and/or corporations that will implement these technologies. The question is first and foremost to be explored empirically "following the actors" (Latour 2005), ie. to empirically (ethnographically) observe how the new constellations evolve and stabilize (or not). Alongside this we also propose conceptual analysis (philosophical and legal), more aligned with democratic and constitutional theory. The question here is to what extents the relevant developments can be described as "constitutional" actions and/or developments. Specifically, we talk about constitutionality in a broad sense (Jasanoff 2003, 2011a, b), as putting things together in new ways, and in relation to the following developments: 1) the coming together of the traditionally separate domains of law and science/engineering, whose working assumptions and methods are quite distinct but now expected to work together; 2) the implementation of ICTs into new environments such as disaster areas and electricity grids; 3) broad developments enabled through ICTs that work across traditional separations between nature and culture (including law).

We envision that "radical interdisciplinarity" will potentially take all of the following shapes, depending on the nature of (the) ensuing project(s): 1) publications resulting from interdisciplinary collaborations but themselves situated inside the relevant disciplines; 2) the same investigations will lead to interdisciplinary joint results and publications across natural and human sciences, and engineering; 3) the project will also have as its aim to go beyond 1) and 2) and experiment with the making of new prototypes into privacy by design, in which the competencies from human and social sciences are actively used by engineers, software developers and others (end users).

Main goal of the project: the main goal of this initiative is to bring together an interdisciplinary group of researchers and practitioners to write research proposals addressing the research question.The research proposals are intended for the EU (Horizon 200, Social Sciences and Humanities, Securities program), Norwegian calls (SAMKUL, ICTs program, Security/Risk program).

Subsidiary goals: The workshops to be arranged will themselves be used to explore the research question. Results from the workshops will be used for the writing of a report to SAMKUL and the Norwegian Research Council concerning fundamental rights in ICTs, as pertains to new and emerging practices such as privacy by design, data protection and privacy impact assessments (DPIAs and PIAs), and especially as concerns the contexts of disaster management and smart meters (smart grids). As

such, the report will argue in favour of the expansion of SAMKUL perspectives into other (large-scale) programmes of the Norwegian Research Council.

Planned activities: The project is scheduled to last for two years, encompassing within that time period three workshops to which all relevant partners (see below) will be invited. In addition the project will result in a report into the proposed topic, scheduled to require 1 person month for a researcher (ie. Kjetil Rommetveit). We do not at this stage provide descriptions of the workshops in greater detail, but plan for flexibility in accordance with changing calls: Horizon 2020 will change for the period of 2016 -2017, as will the priorities of the national Research Councils. Each workshop is scheduled to last for one whole day. The first half of the day will be devoted to discussions of relevant developments of relevant calls as well as relevant developments (technological, political, legal, etc.) relating to the call; the second half will be used for collective writing and brain-storming.

Partners and participants: The project will be lead by researcher **Kjetil Rommetveit**, (SVT - Center for the study of the sciences and humanities, University of Bergen). The SVT is a main hub for studies of science-society interactions in Norway and Europe. The main responsible partners for arranging the workshops will be **Kjetil Rommetveit, Kristrún Gunnarsdottir (Lancaster University) and Niels van Dijk (Vrije Universitait Brussels).** The core group will be supported by Prof. **Brian Wynne**, Lancaster University, who is a leading scholar in the field of risk, the public dimensions of science and technology, and science and technology studies; by Prof. **Mireille Hildebrandt** is Professor of Smart Environments, Data Protection and the Rule of Law at the Institute of Computer and Information Sciences at Radboud Universiteit Nijmegen, Netherlands. She is one of the main promoters of privacy by design in Europe; Prof. **Serge Gutwirth** (Vrije Universitait Brussels) is a leading scholar on privacy and data protection as seen from the points of view of law and science and technology studies. Prof. **Bruna De Marchi** (Center for the study of the sciences and humanities) is a leading sociologist into disasters, risk and science-for policy. These researchers already have proven track-records of working together in interdisciplinary projects, including with engineers, scientists, privacy engineers and policy makers (ie. FP7 projects TECHNOLIFE and EPINET) (Rommetveit, Gunnarsdottír et al. 2013, Gunnarsdottír and Rommetveit, forthcoming), including into data protection impact assessments (van Dijk, Gellert, Rommetveit, forthcoming). At this stage we have not obtained conformations from other partners. In the following we mention main relevant partners to be included in the workshops. All of these are connections that build on going and previous collaborations:

Prof Kai Rannenberg, is a researcher on mobile business and multilateral security, Göethe University, Germany; **Marc Langheinrich** is head of the research group on ubiquitous computing at Università della Svizzera Italiana (USI) in Lugano, Switzerland.; **George Danezis** is reader in Security and Privacy Engineering at the Information Security Group of the Computer Science department at University College London; **Philippe Bonnet** is associate professor at IT University of Copenhagen and an experimental computer scientist focused on building/tuning systems for performance and energy efficiency. **Dr. Monika Büscher** (senior lecturer, Lancaster University) does research on the informationalization of large-scale multi-agency emergency response, especially social media-based public engagement, agile and 'whole community' approaches to disaster response, data

sharing, data protection and privacy. Dr **Dr. Lucy Easthope**, specialises in Disaster Management. She has advised governments, corporations and relief agencies in the aftermath of major incidents, including the 2010 and 2011 Christchurch earthquakes in New Zealand. In addition we shall extend invitations to the following institutions:

Royal Military Academy, Belgium; **Federal Public Service Health**, **Department of Disaster Management** (FPS Health), Belgium; **Belgian Nuclear Research Centre** (SCK-CEN), Belgium; **European Organisation for Security and Cooperation in Europe** (OSCE), Belgium; **UK Ministry of Defence**, **Norwegian Ministry of Defense**; **Intelligent Systems Research Laboratory**, University of Reading, UK; **Institute for Systems Analysis and Computer Science** (CNR), Italy; **Institute of Technology** (KIT), Karlsruhe, Germany.

References
Bundesverfassungsgericht, 2008. 1 BvR 370/07, Absatz-Nr. (1 - 267).
Cavoukian, A., others, 2009. Privacy by design: The 7 foundational principles. Inf. Priv. Comm. Ont. Can.
Flanagan, M., Howe, D., Nissenbaum, H., 2008. Embodying Values in Technology: Theory and Practice, in: van den Hoven, J., Weckert, J. (Eds.), Information Technology and Moral Philosophy. Cambridge University Press, Cambridge, pp. 322–353.
Gambatese, J., Hinze, J., 1999. Addressing construction worker safety in the design phase: Designing for construction worker safety. Autom. Constr. 8, 643–649.
Hes, R., Borking, J., 1995. Privacy-enhancing technologies: the path to anonymity. Registratiekamer and Information and Privacy Commissioner of Ontario., Netherlands.
Hildebrandt, M., 2011. Legal Protection by Design. Objections and Refutations. Legisprudence 5, 223–248.
Iachello, G., Abowd, G.D., 2005. Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 91–100.
Jasanoff, S., 2003. In a Constitutional Moment: Science and Social Order at the Millennium, in: Joerges, B., Nowotny, H. (Eds.), Social Studies of Science and Technology: Looking Back, Ahead, Yearbook of the Sociology of the Sciences. Kluwer, Dordrecht, pp. 155–180.
Jasanoff, S., 2011a. Constitutional Moments in Governing Science and Technology. Sci. Eng. Ethics 17, 621–638. doi:10.1007/s11948-011-9302-2
Jasanoff, S., 2011b. Introduction: Rewriting Life, Reframing Rights, in: Jasanoff, S. (Ed.), Reframing Rights: Bioconstitutionalism in the Genetic Age. MIT Press.
Leenes, R., 2010. Hard lessons. Apology for technology as a regulatory tool. Universiteit van Tilburg, Tilburg.
Lessig, L., 2006. Code 2.0. Basic Books, New York.
Nordmann, A., 2009. European experiments. Osiris 24, 278–302.
Rommetveit, K., Gunnarsdóttir, K., Jepsen, K. S., Bertilsson, M., Verrax, F. and Strand, R. (2013): "The Technolife Project: An experimental approach to new ethical frameworks for emerging science and technology", The International Journal of Sustainable Development.
Van Dijk, N., Gellert, R., Rommetveit, K., 2015. A Risk to a Right? Beyond Data Protection Risk Assessments. Submitted Comput. Law Secur. Rev.