Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Thinking of data protection law's subject matter as a complex adaptive system: A heuristic display

Kunbei Zhang[*], *Aernout H.J. Schmidt*

eLaw@Leiden, Centre for Law in the Information Society, Leiden University, the Netherlands

Keywords:
Data protection law
Complex adaptive system
Dynamics of innovation
Self-organization
Emergence

ABSTRACT

According to both whistle blowers and public reports, some commercial and governmental practices concerning personal data do not even appear to notice the law as a regulatory force. We are not satisfied by what mainstream legal scholarship has on offer in this context. Positivists consider the issue outside their domain. Realists (including their critical branch) focus on the behavior of legal institutions, ignoring many of the diverse institutions that have regulatory force. We need an additional, complementary perspective to help us, legal scholars, earn and hold serious positions in the diverse disciplinary teams that we need to participate in, in order to adequately investigate (and inform on) persistent problems concerning personal-data protection as faced by legislators.

In this article we investigate whether the subject matter of data protection law, identified as Personal Data Community (hereinafter PDC), can be treated as a complex adaptive system (hereinafter CAS). This proposition is premised on the argument that the PDC exhibits key traits of CAS, including systemic, dynamic and complex characteristics. And we further show how complexity theory can help legal scholarship (without losing its identity) to join and add value to diverse disciplinary research and advisory teams. In this article, we aim for a stepping-stone (establishing that data protection law addresses a complex adaptive system with all of its corollaries), rather than for final solutions.

1. Introduction

On May 20th 2013, a former Central Intelligence Agency employee and former National Security Agency Contractor, Edward Joseph Snowden revealed insider information on Internet surveillance programs such as PRISM, Xkeystone and Tempora, as well as on the interception of US and European telephone meta-data.[1] Snowden's disclosure caused a great stir, and a moral panic[2] ensued. American feelings on privacy

* *Corresponding author*. Centre for Law in the Information Society, Leiden University Kamerlingh Onnesgebouw, Steenschuur 25, 2311ES Leiden, the Netherlands.
E-mail addresses: k.zhang@law.leidenuniv.nl, kunbeizhang@outlook.com (K. Zhang), a.h.j.schmidt@law.leidenuniv.nl, aernout.schmidt@gmail.com (A.H.J. Schmidt).

[1] The Snowden Wikipedia page provides a record of some important debates in America on data protection and the NSA. More information about the event is provided at http://en.wikipedia.org/wiki/Edward_Snowden#cite_note-Hill.2FPoll-333. Moreover, The Guardian, one of the first media that got access to the news, made available a timeline that describes the unfolding of the Snowden Story (see Gidda (2013)).

[2] As defined and described in Cohen (1972).

http://dx.doi.org/10.1016/j.clsr.2015.01.007
0267-3649/

and data protection were battered in this storm.[3] The after-effects of the event, directed against American legal practices over both data-protection and public-security issues, followed each other in quick succession. On October 29, 2013, a complete proposal for new legislation was submitted to the House Judiciary Committee. The legislative proposal aimed to end the bulk collection of American communication records and to better balance security and privacy.[4] Moreover; cases were filed to courts, with varying outcomes. In one case, US Federal Judge Richard J. Leon ruled that bulk collection of American telephone metadata likely violates the Constitution of the United States.[5] Yet in another, comparable case, Judge William Pauley ruled differently.[6] Dealing with personal data has become complex and adjudication of these dealings is no longer what we crave for in our legal systems: straightforward and simple.

Media and modern communication facilities encouraged the panic to grow and be transmitted across borders. NSA's practices caused significant discussion in Europe.[7] The reputations of European data protection institutions suffered plenty.[8] The heat produced by Snowden's revelations threatened to blemish the European legal system over data protection, which until then had freely flaunted its banners of strict and comprehensive protection.[9] Its flaw was found in practice since its institutions accomplished nothing, apart from adopting the role of witness to what has been described as "a systematic breach of people's fundamental rights."[10] As a result some future tightening of provisions in the Data protection regulation may occur, perhaps even with some impact on how the U.S.–EU differences concerning legal data protection will be handled.[11] From Asia, since Snowden's first hideout was in Hong Kong, China was inevitably dragged in. China has in the mean time warned that revelations of electronic surveillance on a huge scale by American intelligence agencies will "test developing Sino-US ties" and exacerbate their already "soured relation-ship" on cyber security.[12]

When we wrote this paper, the dust of the storm appeared to have settled a bit. Yet, data protection law was still having a hard time. Concerns on privacy had attracted people to reconsider current legal institutions.[13] Several proposals to fix the data protection laws have been inspired by the panic mentioned. These proposals, together with current data protection laws are striking illustrations of how policy makers attempt and have attempted, through laws, to tame "situations." What is to be tamed are not personal data, but people's individual and collective behaviors related to personal data. Through the lens of legal scholarship the subject matter evokes the need for several perspectives.

In this article we argue that traditional perspectives are insufficient to address these questions in (or in order to help prevent) turbulent times. We show that the complexity perspective may provide at least part of the additional insights required. We first explain why we address the possibilities of complexity theory (Section 2) and subsequently sketch the networked character of the community that is addressed by personal-data protection laws (Section 3) and name it the PDC. In order to be able to decide on the applicability of complexity theory, we first list a set of essentials that define its subject matter, complex adaptive systems (CASs, Section 4). Then we analyze the PDC, and identify it as a CAS (Section 5), our most important result. In Section 6 and Section 7 we provide some considerations for further research into the exploration of combining complexity theory and legal scholarship.

Before entering into the analysis, it is useful to clarify three issues.

First: we do not consider any individual law, treaty or institution to be our main subject matter. Instead, we look at the global cluster of personal-data users, as a whole. We consider it to be at the core of legal scientific ethos to strive for improved understanding of what legal rules and institutions will accomplish when goal-directed laws have to be designed (by the legislator) and upheld (by government agencies and the general public) while facing the possibilities of unforeseen contingencies and incomplete or false information.

[3] For instance, according to Rieder (2013) Snowden's disclosure sparked debates over finding the right balance between national security and civil liberties, while complaints were directed at Obama and his enthusiasms for security and his indifferent attitudes towards privacy and data protection. According to AFP (2013), American spy chief James Clapper stated that "some of the debate ... probably needed to happen," referring to the debate about the best way to balance spy empowerment and privacy protection. He was candid enough to suggest that security agencies had lost the citizens' trust and confidence on privacy protection issues and related care for confidentiality. And according to Neff (2014), USA TODAY and the Pew Research Center conducted a poll surveying American attitudes towards NSA's data collection practices. 1504 adults joined the poll. In July 2013, half of them supported the NSA programs. By January 2014, the percentages had dropped to 40.

[4] See Risen (2013).

[5] Klayman V Obama, Civil Action No. 13-0851 (RJL) United States District Court District of Columbia, DEC 6, 2013.

[6] American Civil Liberties et al. V James R. Clapper, et al Civil Action No. 13-3994 (WHP). United States District Court Southern District of New York. DEC 27, 2013.

[7] In Germany, the data protection commissioner expects the Federal Government to do its best to provide protection against access to citizens' data by third parties and asks the Government to aim for tougher European privacy rules that will prevent the occurrence of similar incidents Scuppert (2013). In France, the International Federation of Human Rights Leagues (Fédération Internationale des Ligues des Droits de l'Homme) and the French League for the Defence of Human Rights (Ligue Française pour la Défense des droits de l'Homme et du Citoyen), filed a motion to open a criminal investigation regarding the incidents disclosed by Snowden dDe Souza (2013).

[8] The Snowden disclosure attracted Brussels' flash points. On October 17, the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE"), released a draft Regulation to replace the original draft prepared by the EU Commission in January 2012. The currently adopted draft aims to establish "high data protection standards" that will be enforced consistently across the EU. It is easy to establish that the new draft was influenced by the Snowden disclosure incident, since it includes a prohibition against telecommunications and Internet companies transferring data to other countries' governmental authorities unless otherwise permitted by EU law Firmer (Firmer, 2013).

[9] See Jentzsch (2003): 2 & 12.

[10] See Rettman (2013).

[11] See Hakim (2013).

[12] See Murray (2013).

[13] Previous footnotes showed that the NSA scandal does change the future of the data protection domain.