Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

A vision for global privacy bridges: Technical and legal measures for international data markets

Sarah Spiekermann, Alexander Novotny *

Vienna University of Economics and Business, Department of Information Systems and Operations, Vienna, Austria

Keywords:
Information privacy
Personal data market
Economics of personal information
Privacy regulation

ABSTRACT

From the early days of the information economy, personal data has been its most valuable asset. Despite data protection laws and an acknowledged right to privacy, trading personal information has become a business equated with "trading oil". Most of this business is done without the knowledge and active informed consent of the people. But as data breaches and abuses are made public through the media, consumers react. They become irritated about companies' data handling practices, lose trust, exercise political pressure and start to protect their privacy with the help of technical tools. As a result, companies' Internet business models that are based on personal data are unsettled. An open conflict is arising between business demands for data and a desire for privacy. As of 2015 no true answer is in sight of how to resolve this conflict. Technologists, economists and regulators are struggling to develop technical solutions and policies that meet businesses' demand for more data while still maintaining privacy. Yet, most of the proposed solutions fail to account for market complexity and provide no pathway to technological and legal implementation. They lack a bigger vision for data use *and* privacy. To break this vicious cycle, we propose and test such a vision of a personal information market *with* privacy. We accumulate technical and legal measures that have been proposed by technical and legal scholars over the past two decades. And out of this existing knowledge, we compose something new: a four-space market model for personal data.

"Only those who know the goal, find the way" Laotse (604 BC–531 BC).

1. Introduction

"Personal data is the new oil of the Internet and the new currency of the digital world" (2011). With these words Meglena Kunewa, Europe's prior commissioner in chief of consumer protection, expressed a current economic reality. Personal information (hereafter abbreviated as "PI") is at the core of online business models: it is regarded as the Holy Grail to gain the attention of users (Brynjolfsson and Oh, 2012). It also drives innovation because it promotes a better understanding of customer needs and reduces corporate cost and risks. Drawing on the analytics of Big PI Data, businesses try to avoid targeting the wrong customers, running into credit defaults, or hiring the wrong staff. Due to these benefits, the Boston Consulting Group predicts that the economic use of PI

* *Corresponding author*. Vienna University of Economics and Business, Department of Information Systems and Operations, Welthandelsplatz 1, D2, 1020 Vienna, Austria. Tel.: +43 1 31336 5279; fax: +43 1 31336 905279.
E-mail address: alexander.novotny@wu.ac.at (A. Novotny).
http://dx.doi.org/10.1016/j.clsr.2015.01.009

can deliver up to € 330 billion in annual economic benefit for organizations in Europe by 2020 (Bcg, 2012). The use of PI and its availability in emerging PI markets follow the predictions of neoclassical economic theory, which says that complete information and transparency creates economic efficiency (Posner, 1978).

However, the strive for economic efficiency is challenged. People's legal right to keep their PI private and their right to informational self-determination (at least in Europe) limit marketers' push for the unrestricted flow and use of PI. Across the globe, regulators and human rights activists that see people's identities commercialized fight the "glass human being". Across jurisdictions a delicate balance needs to be found between peoples' human right to privacy and data protection on one side and economic efficiency on the other (Wef, 2012).

To date, this balance has not been found. From a natural and legal point of view, only customer relationship holding institutions (hereafter abbreviated as "CR-H" for "Customer Relationship Holders") should actually be entitled to use PI for the legitimate purpose of delivering agreed-upon services to customers. However, because PI is such an enticing tradable asset a plethora of data brokers have emerged to pursue more or less legitimate PI trade. An impressive "shadow market" (Conger et al., 2013, p. 406) for personal data has evolved that benefits from a current lack of global technical standards for controlling and auditing data flows. Nobody knows for sure who shares which PI with whom, in what form and on what occasions. Besides this nontransparent distribution structure of the PI market, data collection is mostly happening invisibly, without the full knowledge and true consent of customers (Angwin, 2012).

This status quo is unsatisfactory for all market actors involved. Customers and data protection authorities have reason to complain because they see the legal promise of informational self-determination and privacy increasingly eroded. For CR-Hs, the PI market lacks transparency and fails to create the necessary accountability and trust that is required for creating a predictive market environment. The markets' shadow existence undermines its own long-term viability, making all its players operate at the edge of what is ethically sustainable. A lack of accountability and transparency leads to an arbitrary valuation of the PI asset. And, as we will argue, it also fosters market concentration and impedes service innovation. Finally, different approaches to privacy regulation in the U.S., Europe and Asia lead to tensions that threaten data exchange.

Against this background, we strongly believe that a solid new vision is needed for how the PI market can work efficiently while providing privacy protection and informational self-determination. We don't think that global PI markets can simply muddle along with some technical and legal measures and compromises here and there. Instead we need a PI market, where

- companies handle PI transparently and accountably,
- long-term consumer trust is ensured,
- concentrated PI monopolies (or oligopolies) are broken up to make information more accessible to more companies on a global basis,
- and informational self-determination and privacy of customers is ensured.

If this is the goal, what legal measures would need to be taken? And what technical standards would be needed to enable these legal measures?

The contribution of this paper is that it provides a specific analysis how privacy-enhancing technologies and privacy/data protection law could together balance the right to privacy with market efficiency in order to create a trustful PI market. We present a vision of technical and legal bridges between continents that could be used by information systems and computer science researchers, standardization bodies and policy makers to challenge, streamline and prioritize current privacy regulation initiatives and technical developments. We believe that such a vision is a highly important tool, because what we need in this field is direction. As Laotse said once: "Only those who know the goal find the way". Many aspects of the goal to have privacy-friendly digital services have been described already. Over two decades, legal and technical scholars in the field of data protection and privacy have dedicated their scientific lives to propose solutions to various aspects of privacy-friendly markets. Our aim in this article is to bundle the voices of these scholars into a chorus and to show how their solutions can be put together and integrated into one vision picture.

So far, only a few scholars have theorized about how a PI market vision could be organized with privacy in mind (Laudon, 1996; Noam, 1997; Schwartz, 2003; Aperjis and Huberman, 2012). These scholars have typically envisioned a market where people legally own and control their data, selling PI usage rights to data brokers under various organizational conditions. However, their proposed models fail to grasp the complexity of today's data handling practices; including the grown power structure of data markets. They hardly integrate the existing technological and legal landscape. And they provide no pathway to empower customers.

This article takes a different approach. We embrace existing work in the field of privacy research and outline how it could be leveraged in the current economic and technical environment. We show how privacy-enhancing technologies that allow for accountability (Pearson and Mont, 2011), agent-based privacy preference management (e.g., Cranor et al., 2006), cloud computing (e.g., Pearson and Charlesworth, 2009), anonymization (e.g., k-anonymity (Sweeney, 2002)), and differential privacy (Dwork, 2006) could be used to turn around today's adverse PI market situation. We think about incentives of current actors to participate in the market vision we propose. And we argue that only a symbiosis of "code and law" (Lessig, 2006) can produce an efficient PI market where customer rights to privacy are maintained.

To develop our PI market vision, we initially proposed a 3-tier market model (Novotny and Spiekermann, 2013) that categorized current PI market players into three groups: (1) CR-Hs involved in direct service- and PI exchange with customers, (2) data processing companies servicing CR-Hs and (3) third parties (including data brokers), which would work purely on anonymized data. This model was critically discussed and challenged in the course of 13 in-depth interviews with world-leading data protection experts (denoted hereafter