Zeitschrift: Zeitschrift für schweizerisches Recht = Revue de droit suisse = Rivista di diritto svizzero = Revista da dretg svizzer : Halbband II. Referate und Mitteilungen des SJV

Herausgeber: Schweizerischer Juristenverein

Band: 134 (2015)

Artikel: Perspectives on the Future of Digital Privacy

Autor: Gasser, Urs

DOI: https://doi.org/10.5169/seals-895807

Perspectives on the Future of Digital Privacy

URS GASSER*

* Dr. iur., LL.M. (Harvard), Professor of Practice, Harvard Law School; Executive Director, Berkman Center for Internet & Society at Harvard University. Contact: ugasser@law.harvard.edu. I am grateful for the research support by my colleagues at the Berkman Center and the Research Center for Information Law at the University of St. Gallen, as well as for inspiring conversations with the students in my Spring 2015 Comparative Online Privacy Seminar at Harvard Law School. All sources last accessed on April 24, 2015.

Contents

A. Framing the Digital Privacy Challenge

I. Introduction

Over the past decade, the end of privacy has been predicted multiple times, most recently on the cover of the well-respected *Science Magazine*.[1] Judging from the daily headlines in various news outlets, expert discussions on TV, and increased calls for tougher privacy laws and enforcement across the world, privacy in the digitally networked age is at the very least under severe stress.[2] Whether the latest revelations about excessive data collection practices by foreign or domestic national security authorities,[3] apparently weekly data leaks through which millions of customer data points are revealed,[4] or the aggressive tracking practices by marketing firms of every online click or app use on our phones,[5] privacy intrusions and violations seem to have become endemic as the adoption of digital technologies has spread across continents.[6] In the post-Snowden world[7] and in the age of multi-billion dollar companies such as Google and Facebook, whose business models are based on advertisements, privacy – if not dead – is in critical condition.

In light of what one might call the *digital privacy crisis*,[8] this report examines the *future* (rather than the end) of privacy in the digital world. More specifically, the focus of this contribution is on privacy issues that emerge in the *relationship between users and companies* that collect, aggregate, analyze, and

---

1 Martin Enserink and Chin Gilbert, The End of Privacy, Science 347, No. 6221, pp. 490–491, January 30, 2015.

2 See, e.g., Alex Preston, The Death of Privacy, The Guardian, August 3, 2014. <http://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston>.

3 Loek Essers, UK Government's Spying Practices Challenged at European Human Rights Court, PCWorld, April 10, 2015. <http://www.pcworld.com/article/2908752/uk-governments-spying-practices-challenged-at-european-human-rights-court.html>.

4 See, e.g., 2015 Data Breach Investigations Report (DBIR), Verizon, 2015. <http://www.verizonenterprise.com/DBIR/2015/>.

5 See, e.g., Mitch Lipka, A New Worry for Consumers: Cross-Device Tracking, CBS News, March 19, 2015. <http://www.cbsnews.com/news/determining-the-risks-of-cross-device-tracking/>.

6 See, e.g., Internet Users (per 100 People), The World Bank, n.d. <http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=default>; Social Networking Fact Sheet, Pew Research Center, 2014. <http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/>; Social, Digital, and Mobile in Europe in 2014, We Are Social, February 2014. <http://wearesocial.net/tag/europe/>.

7 Aaron Blake, Welcome to the Post-Edward Snowden Era, The Washington Post, September 11, 2014. <http://www.washingtonpost.com/blogs/the-fix/wp/2014/09/11/welcome-to-the-post-edward-snowden-era/>.

8 A brief note on terminology: The term «digital privacy» is used as a short-cut throughout the report to refer to the information privacy or, in European terminology, data protection concerns and challenges that have and will emerge in the digitally networked environment that is characterized by the rise of «Big Data» and the «Internet of Things,» as further described in the next section. The terms «personal data» and «personally identifiable information» are used interchangeably, depending on context.

use data.[9] Privacy challenges vis-à-vis governments in general and national security agencies in particular have dominated the privacy debate over the past year, producing a vast amount of literature and triggering legal reform discussions across many countries and international fora. Meanwhile, the threats in the consumer privacy space – absent a Snowden-equivalent privacy meltdown – are arguably less transparent and more complex, considering the vast number of actors involved, the distributed nature of the relevant processes, and centrifugal forces at play. This contribution, with its focus on the *private sector,* seeks to map the respective challenges and opportunities concerning digital privacy.

This report takes a *phenomenon-oriented* and – for a continental European legal audience – perhaps unorthodox methodological approach.[10] First, it offers observations on digital privacy from cross-jurisdictional perspectives in the sense that it includes (and sometimes contrasts) real-world examples, developments, forces, and actors as well as references to digital privacy legislation and regulation in the private sectors within the United States, Europe, and Switzerland. Although the approach is not necessarily comparative, it invites an exploration of similarities and differences, which is helpful for understanding the global dynamism of the topic. Particular emphasis is put on developments in the US that are relevant across the Atlantic – such a view might offer interesting insights at a time when information flows are increasingly global, and when the Internet space for users is significantly shaped and often dominated[11] by US technologies, companies, and commercial practices, as further discussed below.[12]

Second, the article crosses not only traditional methodological and jurisdictional boundaries, but also *disciplinary* ones. The core argument of the report is that the current digital privacy crisis and resulting challenges need to be *seen in context and as part of deeper-layered tectonic shifts* in the ways in which infor-

---

9 For an overview of the different relationships in data protection or information privacy law, see, e.g., Kai von Lewinski, Die Matrix des Datenschutzes, Tübingen 2014.

10 The methodological perspective is shaped by the author's work and collaborations on two continents, and heavily influenced by the Information Law Approach, see Herbert Burkert, Information Law: From Discipline to Method, Berkman Center Research Publication No. 2014–5, February 28, 2014. <http://papers.ssrn.com/abstract=2402866>; and Urs Gasser, Informationsrecht in «E»-Umgebungen, Information Law in eEnvironments, pp. 7–24, Zurich 2002; as well as shaped by the interdisciplinary research and teaching activities at the Berkman Center for Internet & Society, a university-wide center at Harvard — and particularly informed by the framework of interoperability, see John Palfrey and Urs Gasser, Interop: The Promise and Perils of Highly Interconnected Systems, New York 2012. For context, see Jens Drolshammer, Globalization and the Law of Information, in: Thomas Cottier and Jens Drolshammer (eds.), The Anthology of Swiss Legal Culture, n.d. <http://www.legalanthology.ch/>.

11 Matthiew Pelissie Du Rausas, James Manyika, Eric Hazen, Jacques Bughin, Michael Chui and Remi Said, Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity, McKinsey & Company, May 2011, p. 4. <http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters>.

12 See, e.g., Shawn M. Powers and Michael Jablonski, The Real Cyber War: The Political Economy of Internet Freedom, Urbana 2015.

mation is created, shared, accessed, and used in the globalized digital world. These shifts, in turn, are the result of a complex interplay among technical, economic, behavioral and normative forces. Interdisciplinary knowledge is not only needed to better understand and analyze the origins and dimensions of today's privacy crisis, but is also required when mapping the *solution space* and considering the future of digital privacy, especially from a legal and policy perspective and in the sense of a mixed governance approach.[13]

With these objectives and parameters in mind, the report begins framing the digital privacy challenge by outlining two particularly trending phenomena that arguably best characterize the complexities, unpredictability, and pervasiveness of the digital privacy challenge: the rise of Big Data and the Internet of Things. The brief discussion of these two leading use cases sets the stage for an overview of some of the key privacy-related concerns and challenges in the consumer space as far as cutting-edge digital technologies are concerned. The use cases will also serve as reference points throughout the report when illustrating and evaluating the different possible approaches to the future of digital privacy.

Based on this framing and still from a phenomenological perspective, the second part of the report examines the key technical, economic, behavioral and – to some extent – legal forces that are at play and need to be taken into account when analyzing the current landscape, mapping possible responses to the crisis, and exploring the future of digital privacy. As in all other parts of this article, this section offers only *perspectives* rather than a comprehensive analysis of all possible factors and dimensions of the problem, for the purposes of inviting further conversation and investigation across disciplines and geographies.

The third and main section of the report maps and discusses – following a broader governance rather than a strictly law-focused approach – the different responses to the digital privacy crisis by examining four different response modes, which build upon the standard «toolbox» of cyberlaw.[14] First, technological approaches such as Privacy Enhancing Technologies and Privacy by Design are considered. Second, the report discusses the possible role of market forces and other market-based mechanisms – such as the reputation of a company – when addressing the privacy challenges of our time. Third, a series of human-centered responses to the privacy crisis are discussed, ranging from user education and empowerment to concepts derived from behavioral economics, such as nudging. Finally, traditional and non-traditional legal approaches are examined as a way to not only address the digital privacy crisis, but also potentially coordinate or shape the other governance mechanisms discussed in this section.

---

13 On the different modes of regulation in the digital age see, e.g., Lawrence Lessig, Code: And Other Laws of Cyberspace, New York 1999.

14 See, e.g., Rolf H. Weber, Realizing a New Global Cyberspace Framework: Normative Foundations and Guiding Principles, Zurich 2014.

The report ends with a series of observations and suggestions regarding the future of digital privacy and highlights the importance of the legal system. Ultimately, this contribution concludes that there is no silver bullet solution and instead explores the contours of a *framework for blended governance*, necessitated by a highly interconnected, complex, and uncertain world in which the role of information – including personal data – and the importance of information flows will only increase over time.

II. Guiding Use Cases

1. Big Data

The term «Big Data» describes a phenomenon in which vast amounts of information are collected, pooled, and analyzed to provide empirical insights that help explain the present and the past, and predict the future. While it lacks a universally-agreed upon definition,[15] Big Data is generally described as «datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze.»[16] Scholars characterize Big Data with the terms *«more, messy, and correlations,»* indicating that the size of the datasets is only one aspect of the phenomenon, as quantitative and qualitative characteristics are intertwined.[17] The amount of information, for instance, can to an extent overcome the issues associated with lower quality (or «messy») data in smaller quantities – the more data analyzed, the more accurate the results.[18] The ability to identify correlations and patterns is also key, and provides a powerful tool for answering questions that were not asked – or perhaps not even conceived – when the data was collected. Algorithms can be used to identify hidden patterns between pieces of information thought irrelevant or too complex to analyze and make predictions about future behaviors with surprising accuracy;[19] although correlations do not explain the causal links, they provide substantial insights into how individual elements interact and behave.[20]

---

15 See, e.g., Jonathan Stuart War and Adam Barker, Undefined by Data: A Survey of Big Data of Definitions, Computer Research Repository, 2013. <http://arxiv.org/pdf/1309.5821v1.pdf>.

16 James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh and Angela Hung Byers, Big Data: The Next Frontier for Innovation, Competition, and Productivity, McKinsey & Company, May 2011. <http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation/>.

17 Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution that will Transform how we Live, Work, and Think, New York 2013.

18 Matthew Hindman, Building Better Models Prediction, Replication, and Machine Learning in the Social Sciences. The ANNALS of the American Academy of Political and Social Science 659, no. 1, pp. 48–62, May 1, 2015, p. 53.

19 See, e.g., Hindman (n. 18), pp. 53–55.

20 Foster Provost and Tom Fawcett, Data Science for Business: What you Need to Know about Data Mining and Data-Analytic Thinking, Sebastapol 2013; Eric Siegel, Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, Hoboken 2013.

An *ecosystem* has emerged in the private and public sectors to support users of Big Data – primarily companies in the private sector – with the infrastructure, software platforms, data, and knowledge necessary to take advantage of it. This includes divisions of large technology companies, like Amazon's Web Services division, and startups, such as Cloudera, which provide cloud computing infrastructure and analytics platforms, as well as data sources like Fitbit, Jawbone, open government databases, BlueKai, and Acxiom, and a variety of analytics service and software oriented firms that offer software tools, consulting, and related services.[21]

The *process* of using Big Data involves a series of steps, including aggregation and analysis, which are particularly key to understanding contemporary privacy challenges.[22] After data is collected from a variety of sources – for example, directly from consumers or from private and public third-party sources – it is often refined from its raw form, integrated with other types of data, and prepared for analysis, typically on analytics platforms like Hadoop and MapReduce. During the analytics phase, data scientists may use algorithmic techniques such as machine learning, which uses algorithms that can be trained to accomplish specific tasks such as predictions or image detection, and data mining, which categorizes and summarizes information and identifies patterns.[23] The outputs of these powerful analyses can be used to reveal patterns and correlations, build predictive models to analyze more data, or to make decisions as part of a larger algorithmic or human process, ranging from delivering product recommendations to developing business strategy.[24]

Although it is still in the early days, Big Data has a number of real world *applications* that directly impact consumers, primarily through the private sector where it has been most widely adopted. There is a lack of transparency with respect to Big Data. In part this is due to the complexity of the space, but it is also because many companies do not openly disclose how they use Big Data in detail. However, numerous stories have emerged in the media, in reports from leading consulting firms, and – to some degree – from company sources. The following examples from the insurance, healthcare, retail, and advertising in-

---

21 See, e.g., Eileen McNulty, Understanding Big Data: The Ecosystem, Dataconomy, June 3, 2014. <http://dataconomy.com/understanding-big-data-ecosystem/>.

22 See, e.g., Divyakant Agrawal, Philip Bernstein, Elisa Bertino, Susan Davidson, HP Michael Franklin, Johannes Gehrke, Laura Haas, Alon Halevy, Jiawei Han, H. V. Jagadish, Alexandros Labrinidis, Sam Madden, Yannis Papakonstantinou, Jignesh M. Patel, Raghu Ramakrishnan, Kenneth Ross, Cyrus Shahabi, Dan Suciu, Shiv Vaithyanathan and Jennifer Widom, Challenges and Opportunities with Big Data: A Community White Paper, 2012. <http://www.cra.org/ccc/files/docs/init/bigdatawhitepaper.pdf>.

23 See, e.g., Rob Schapire, COS 511: Theoretical Machine Learning, Princeton University, February 4, 2008. <http://www.cs.princeton.edu/courses/archive/spr08/cos511/scribe_notes/0204.pdf>; Alexander Fumas, Everything You Wanted to Know about Data Mining but Were Afraid to Ask, The Atlantic, April 3, 2012. <http://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/>.

24 See, e.g., Mayer-Schönberger/Cukier (n. 17); Provost/Fawcett (n. 20); Siegel (n. 20).

dustries are intended to give a sense of Big Data's current and future applications:

- *Insurance companies* use Big Data analytics to detect potential insurance fraud and assess risk in policies by identifying patterns of anomalous behaviors based on historical claims and data obtained from external sources.[25] They also use Big Data to help to underwrite individuals previously too risky to insure. For instance, life insurance companies use Big Data analytics to assess data provided voluntarily by high-risk customers, which allows them to monitor these individuals on an ongoing basis, in exchange for an insurance policy that would have been otherwise unaffordable or unavailable.[26]
- The *healthcare industry* is using Big Data to move closer to evidence-based clinical medicine.[27] Traditional approaches to clinical medicine rely heavily on generalizations and heuristics, which are often imprecise on the individual level.[28] However, this is changing now that more health-related data is available from a variety of sources, including electronic medical records, distributed sensors, clinical research studies, and other sources. Big Data promises to help the industry better understand population-level trends, intervention and treatment efficacy, and tailor preventative and reactive care to individuals. According to leading consulting firms, the resulting higher quality of care and improved early intervention could reduce overall costs as much as 12–17% in the US and Europe.[29]
- The *retail and advertising sectors* are also among the early adopters in the Big Data revolution. These sectors are using Big Data collected from in-store and online transactions, cameras, and cell phones of customers who visit stores[30] to optimize the layout of stores, build demand-driven forecast

---

25 See Nilay D. Shah and Jyotishman Pathak, Why Health care May Finally Be Ready for Big Data, Harvard Business Review, 2014. <https://hbr.org/2014/12/why-health-care-may-finally-be-ready-for-big-data>; Eric Brat, Stephan Heydorn, Matthew Stover and Martin Ziegler, Big Data: The Next Big Things for Insurers?, Boston Consulting Group, March 25, 2013. <https://www.bcgperspectives.com/content/articles/insurance_it_performance_big_data_next_big_thing_for_insurers/>.

26 Eric Brat, Paul Clark, Pranay Mehrotra, Astrid Strange and Celine Boyer-Chammard, Bringing Big Data to Life: Four Opportunities for Insurers, Boston Consulting Group, July 17, 2014. <https://www.bcgperspectives.com/content/articles/insurance_digital_economy_Bringing_big_data_life/>.

27 Basel Kayyali, David Knott and Steve Van Kuiken, The Big-Data Revolution in US Health Care: Accelerating Value and Innovation, McKinsey & Company, April 2013. <http://www.mckinsey.com/insights/health_systems_and_services/the_big-data_revolution_in_us_health_care>.

28 Kayyali/Knott/Van Kuiken (n. 27).

29 Silvia Piai, Bigger Data for Better Healthcare, IDC Insights, September 2013. <http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/bigger-data-better-healthcare-idc-insights-white-paper.pdf>.

30 Stephanie Clifford, Attention, Shoppers: Store is Tracking Your Cell, The New York Times, July 13, 2013. <http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html>; Jennifer Valentino-DeVires and Jeremy Singer-Vine, They Know

models to stock shelves, generate product recommendations, and deliver tailored advertising to potential customers.[31] In the US, pharmacy retailer CVS Caremark found data patterns that led them to develop alternative store configurations to serve the profiles of shoppers they deemed most valuable, which can vary greatly store-to-store.[32]

The examples above illustrate some of the *benefits* of Big Data, which holds potential for solving complex problems, improving quality of life, and promoting innovation and prosperity.[33] While much remains to be seen, Big Data is predicted to impact many other fields as well. For example, scholars believe it will transform the natural and life sciences, allowing researchers to ask deeper questions and gain new insights into the behaviors of humans and their surroundings.[34] Big Data is also forecasted to create economic benefits, including more competition, efficiency, cost savings, and new business models; and, individuals will capture the downstream benefits from an improved environment, health and educational systems, and a diverse marketplace with innovative products.

2. *Internet of Things*

While defining the Internet of Things (IoT) is difficult due to its vast scope and constantly evolving nature – and what technologies it encompasses – this phenomenon can be broadly defined as «all devices and objects whose state can be read or altered via the Internet.»[35] The falling costs of electronic storage and processing power – in addition to developments in Big Data, cloud computing, M2M communication, and sensor technology which have led to improved machine learning,[36] and the rising demand for Internet-connected devices – is leading to exponential growth in an array of *devices with sensors, connectivity, and*

What You're Shopping For, The Wall Street Journal, December 7, 2012. <http://www.wsj.com/articles/SB10001424127887324784404578143144132736214>.

31 See, e.g., Stephanie Clifford, Using Data to Stage-Manage Paths to the Prescription Counter, The New York Times, June 19, 2013. <http://bits.blogs.nytimes.com/2013/06/19/using-data-to-stage-manage-paths-to-the-prescription-counter/>.

32 Clifford (n. 31).

33 See, e.g., Liran Einav and Jonathan D. Levin, The Data Revolution and Economic Analysis, National Bureau of Economic Research Working Paper 19035, Cambridge 2013. <http://www.nber.org/papers/w19035.pdf>; David Benady, Can Big Data Improve the Lives of People in the Developing World?, The Guardian, December 11, 2014. <http://www.theguardian.com/sustainable-business/2014/dec/11/can-big-data-improve-the-lives-of-people-in-the-developing-world>; Lyndsey Gilpin, How Big Data is Going to Help Feed Nine Billion People by 2050, TechRepublic, May 2014. <http://www.techrepublic.com/article/how-big-data-is-going-to-help-feed-9-billion-people-by-2050/>.

34 Jonathan Shaw, Why ‹Big Data' Is a Big Deal, Harvard Magazine, March-April 2014. <http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal>.

35 OECD Digital Outlook 2015 – Chapter 5: Emerging Issues: The Internet of Things. OECD, March 20, 2015, pp. 6–8 (forthcoming, on file with author).

36 OECD (n. 35), p. 7.

processing capabilities. These devices monitor a wide variety of activities and phenomenon, from health and fitness metrics, location, the state of the environment, food quality, and «much else that would not be considered a thing per se.»[37] Collectively referred to as the Internet of Things, these intelligent, sensing devices promise to make technological systems more efficient and adaptive to individual behavior and needs.

Platforms are being developed by companies such as Samsung, Google, and Apple to support an array of devices that promise to make homes safer, more energy efficient, and more adaptive to individual behavior and needs. Among the most widely adopted smart devices are vehicles with built-in sensors that automatically detect a collision and transmit information about the location and severity of the accident to emergency responders,[38] thermostats that automatically adjust based on the time of day and whether anyone is home,[39] and public trash receptacles that notify local waste management when they reach capacity.[40] In addition, new applications for the Internet of Things are continuously being deployed in sectors as diverse as consumer goods, healthcare, retail, manufacturing, transportation, agriculture, waste management, and security and public safety.[41]

As the term Internet of Things implies, the *ubiquity* of these technologies is leading to an evolution of the Internet into a global network composed of not only computers but also of interconnected, sensing objects. While predictions as to the actual size and rate of growth of the Internet of Things vary, several sources estimate that there will be roughly 50 billion interconnected IoT devices by 2020.[42] Given this rapid expansion, a new information service architecture is developing to meet the demands of these devices.[43] The Internet of Things relies on a range of different types of embedded sensors, controllers, and systems; cloud-based computing services; and data communication tools

---

37 OECD (n. 35), p. 4.

38 See, e.g., Stefan Rauscher, Jeffrey Augenstein, George Bahouth and Oliver Pieske, Enhanced Automatic Collision Notification System – Improved Rescue Care Due to Injury Prediction – First Field Experience, Proceedings of the 21st International Technical Conference on the Enhanced Safety of Vehicles, 2009. <http://www-nrd.nhtsa.dot.gov/pdf/esv/esv21/09-0049.pdf>.

39 See, e.g., Energy Savings from the Nest Learning Thermostat: Energy Bill Analysis Results, Nest Labs, February 2015. <https://www.nest.com/downloads/press/documents/energy-savings-white-paper.pdf>.

40 See, e.g., Michael B. Farrell, Boston to Install 400 Solar-Powered Trash Cans, Boston Globe, July 14, 2012. <http://www.bostonglobe.com/business/2012/07/13/boston-adds-solar-powered-trash-cans/eOOlBGNoEb6Wfj1Sp9SWNI/story.html>.

41 See generally Mehmet Ersue, Dan Romascanu, Juergen Schoenwaelder and Anuj Sehgal, Management of Networks with Constrained Devices: Use Cases, Internet Engineering Task Force Working Paper, February 14, 2014. <https://tools.ietf.org/html/draft-ietf-opsawg-coman-use-cases-01>.

42 OECD (n. 35), p. 18.

43 See generally Rolf H. Weber, Internet of Things – New Security and Privacy Challenges, Computer Law & Security Review, Vol. 26, No. 1, pp. 23–30, 2010.

and protocols such as Wi-Fi, Bluetooth, radio frequency identification (RFID), and proprietary wireless protocols for specific domains like home automation.[44] The wide variation in technologies and protocols involved poses significant interoperability, scalability, performance, and security challenges for enabling the collection, storage, analysis, and communication of data across a vast number of devices and services of different types.[45]

Internet of Things devices are being introduced to the *consumer marketplace* at a rapid pace, with extraordinary growth in areas such as home automation, wearable technology, and vehicle-based devices. Examples from the US include the following:

- Diverse actors have created platforms for *home automation*, including Google Nest, Staples Connect, Lowe's Iris, Philips Hue, GE Link, and Apple HomeKit. These devices and protocols are marketed to increase energy efficiency, home security, and personal convenience through enhancements to door locks, thermostats, smoke and carbon monoxide detectors, light bulbs and switches, cameras, sprinklers, garage doors, refrigerators, ovens, and washers and dryers.
- Google, Apple, Jawbone, Fitbit, and Nike, among others, are producing smart watches and activity trackers that enable individuals to *monitor* their exercise habits and sleep quality using embedded accelerometers, heart rate sensors, and Bluetooth Low Energy for leveraging a nearby smartphone's GPS and Wi-Fi connectivity for cloud data access and processing capabilities.
- Companies like Tesla are leading the deployment of *smart vehicle technology*, which can send over-the-air software updates to its cars to resolve, for example, suspension and charging issues.[46] Similarly, GM's OnStar offers embedded devices for automatic crash response, turn-by-turn navigation, and vehicle location and unlocking services. Progressive also provides insurance discounts based on users' driving habits, which are recorded by a device connected to a vehicle's diagnostic port.
- Mobile device companies like Google, Samsung, and Apple are leading the development of *interoperable platforms* that integrate their consumer devices and data services with third party home automation and wearable de-

---

44 See generally Carles Gomez and Josep Paradells, Wireless Home Automation Networks: A Survey of Architectures and Technologies, 48 IEEE Communications Magazine, pp. 92–101, June 2010. <http://www.ann.ece.ufl.edu/courses/eel6935_11fal/papers/Survey of home automation networks.pdf >.

45 See Palfrey/Gasser (n. 10), Chapter 13: Architectures of the Future: Building a Better World; Urs Gasser, Interoperability in the Digital Ecosystem, International Telecommunication Union, GSR Discussion Draft, forthcoming 2015.

46 See Alex Brisbourne, Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things?, Wired, February 5, 2014. <http://www.wired.com/2014/02/teslas-air-fix-best-example-yet-internet-things>.

vices.[47] In addition, cloud service providers like IBM, Amazon Web Services, Cisco, and GE are developing Big Data analytics platforms to support IoT devices and applications created by third party developers.[48] An even greater number of companies are developing consumer-facing smartphone apps for combining and interpreting data from smart devices for communications, home automation, navigation, scheduling, health, fitness, and entertainment.

The examples above illustrate the many ways in which the Internet of Things is predicted to bring *gains in efficiency and convenience* to individuals and society at large. The motivation behind home automation, for example, is to bring increased control, predictive learning, and personalization to everyday devices in the home. Wearable devices, to give another example, that combine data with information from other devices and services can enable an individual to monitor and meet personal exercise and nutrition goals, collect health-related data real time, and so on. As smart devices become more common and as their potential uses grow, these benefits will increase and extend to new areas of everyday life. While greater *standardization* and interoperability will need to be ensured before a reliable and widespread Internet of Things ecosystem can be established,[49] in the aggregate, these devices are expected to lead to significant cost savings, more efficient energy consumption, improvements in public health and safety, and advances in scientific research.

3. *Initial Observations*

From the brief use cases, a number of initial observations are useful for understanding the future of digital privacy in the age of Big Data and the Internet of Things. The use cases indicate that privacy and the privacy-related challenges of these phenomena need to be seen against the backdrop of the *larger tectonic shifts* underway.[50] Both the Big Data phenomenon and the Internet of Things are evolutionary products of the new digitally networked environment, fueled by the Internet and the trend towards digitization. Together, they are changing the ways in which information – including personal data – is created, dissemi-

---

47 See Andrew Cunningham, OK Google, Crank the A/C: Nest Announces New Smart Home API, Ars Technica, June 25, 2014. <http://arstechnica.com/gadgets/2014/06/ok-google-crank-the-ac-nest-announces-new-smart-home-api>; Stephen Pulvirent, Samsung's Smart-Home Master Plan: Leave the Door Open for Others, Bloomberg News, January 6, 2015. <http://www.bloomberg.com/news/articles/2015-01-06/samsungs-smart-home-master-plan-leave-the-door-open-for-others>; Aaron Tilley, How Apple HomeKit Is Already Changing the Smart Home Industry, Forbes, September 8, 2014. <http://www.forbes.com/sites/aarontilley/2014/09/08/why-this-smart-device-maker-chose-apple-over-google-in-the-smart-home/>.

48 See, e.g., IBM, IBM Extends Bluemix with Cloud Service for the Internet of Things, Press Release, October 15, 2014. <http://www-03.ibm.com/press/us/en/pressrelease/45102.wss>.

49 OECD (n. 35), pp. 35–36.

50 See, e.g., Jacqueline Lipton, Mapping Online Privacy, Northwestern University Law Review, Vol. 104, No. 2, 2010. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443918>.

nated, accessed, used, and reused by individuals and businesses, as well as at whose discretion and at what cost these actions take place. Additionally, both use cases demonstrate the explosion in the amount of data that is created, processed, and stored, the fast-growing number and variety of actors engaged in the data ecosystem, society's growing interdependence on data, and the increasing technical complexity of the systems and components involved.

The use cases also suggest that these shifts in the information environment, from which the various privacy and privacy-relevant challenges and concerns emerge, are the result of a multi-dimensional *interplay among technical, economic, and behavioral factors*, among others. These factors will be described in detail in a later section. Neither Big Data nor the Internet of Things can be appropriately understood if looked at as merely technological phenomena; rather, they have emerged and continue to evolve in a complex environment with many interacting elements. Further, the examples also indicate the dynamic nature of the overall ecosystem, with technologies, business models, user behaviors, and other key elements in flux. As a result, privacy is a moving target that must be understood in the context of the various forces at play, without a clearly predictable future.

III. Privacy Challenges

Although Big Data and the Internet of Things promise many societal and economic benefits, they give rise to a broad range of significant privacy-related concerns that have been recognized among various stakeholders around the globe, including policy-makers, regulators, consumer associations, and privacy experts. These concerns also mirror many of the broader issues at stake in the digital privacy crisis.

At a high level, both Big Data and the Internet of Things are based on the ability to collect and use *large amounts of fine-grained information*. The sheer volume and personal nature of the information is by itself concerning; however, so too are the abilities of these technologies to learn and capture sensitive details from information that seems innocuous, mundane, or meaningless. When examined at scale, Big Data finds patterns and reveals information that may not be present in the data itself. For example, Target Corporation, a US-based department store-retailer, used Big Data analytics techniques to develop a «pregnancy prediction score» that calculates the likelihood of pregnancy and estimates due dates within a few weeks, all based on purchase patterns around 25 common products, including unscented lotions, cotton balls, wash cloths, and hand sanitizers.[51] The technique is surprisingly accurate and can even find women who do not physically appear pregnant. The purpose of Target's actions

51 Charles Duhigg, How Companies Learn Your Secrets, The New York Times Magazine, February 16, 2012. <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

in this case, which was not necessarily nefarious, was to send households customized advertising to gain loyalty during a moment in life when household brand loyalties and habits are known to change.

The practices behind Big Data and the Internet of Things are frequently *unpredictable* and *opaque* to consumers. Internet of Things devices, for example, often operate within very personal environments, like the home or on an individual's body, replacing familiar analog objects that do not collect personal information with those that do.[52] The data collection occurs without obvious visual cues, and it can be disclosed to other services and devices in ways that are often invisible. As a result, consumers are typically unaware of the full extent to which personal data about them is collected and shared with third parties.[53] One early example of this occurred in August 2014, when a moderate earthquake struck Northern California during the middle of the night. The following day, Jawbone, a company which markets an Internet of Things sensor that tracks sleeping habits, released visualizations illustrating how the earthquake disrupted wearers of its devices within 0, 25, 50, and 100 mile increments from the epicenter.[54] Although the information released in aggregate was not particularly sensitive to individuals, it surprised many users of the devices who were unaware that Jawbone had any access to the data their devices were collecting as they slept.[55]

Concerns like these, as well as many others, have attracted scrutiny from government officials, policy advisors, and other experts. In particular, reports in the US, Europe, and Switzerland highlight a series of privacy and privacy-related *challenges and concerns* around Big Data and the Internet of Things, which can roughly be grouped into the following three categories: (1) challenges for traditional mechanisms aimed at protecting privacy; (2) new or amplified privacy concerns related to the use of personal data; and (3) cumulative effects of such challenges on trust and technology adoption. The following non-exhaustive list of concerns, identified across selected policy documents on both continents, illustrates the breadth and depth of the privacy challenges in each category and associated with the two use cases:

---

52 See generally U.S. Federal Trade Commission (FTC), Internet of Things: Privacy & Security in a Connected World, FTC Staff Report, January 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

53 For a discussion of user privacy perceptions in the context of mobile applications, see Elizabeth Fife and Juan Orjuela, The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security, International Journal of Engineering Business Management, Vol. 4, Special Issue on Digital and Mobile Economy, 2012. <http://cdn.intechopen.com/pdfs-wm/38052.pdf>.

54 Eugene Mandel, How the Napa Earthquake Affected Bay Area Sleepers, The Jawbone Blog, August 25, 2014. <https://jawbone.com/blog/napa-earthquake-effect-on-sleep/>.

55 Sara M. Watson, Ask the Decoder: Did I sign up for a global sleep study?, AlJazeera America, October 29, 2014. <http://america.aljazeera.com/articles/2014/10/29/sleep-study.html>.

Challenges for traditional privacy protecting mechanisms

- *Anonymization and de-identification*: Privacy policy reports in the US[56] and the EU[57] as well as privacy experts in Switzerland[58] have pointed out that anonymization and de-identification – key techniques used to avoid falling into the category of «personally identifiable data» that triggers legal obligations under various privacy laws – are no longer effective in the context of Big Data since it involves so many data points that it may prove too difficult to unlink identities from each piece of data.[59] This has led legal scholars to conclude that all data should be treated as personally identifiable as a matter of good practice.[60]

---

56 Executive Office of the President of the United States, Big Data and Privacy: A Technological Perspective, US President's Advisory Council on Science and Technology, May 2014. <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>; U.S. White House, Big Data: Seizing Opportunities, Preserving Values, May 2014. <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>; U.S. Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, March 2012. <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

57 Article 29 Data Protection Working Party, Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU, Adopted on September 16, 2014. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf>; European Union Agency for Network and Information Security (ENISA), Privacy and Data Protection by Design – from Policy to Engineering, December 2014. <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design>.

58 Bruno Baeriswyl, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Rolf H. Weber and Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, pp. 45–59, Zürich 2014; see also Rolf H. Weber, Big Data: Rechtliche Perspektiven, in: Rolf H. Weber and Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, pp. 17–29, Zürich 2014.

59 See, e.g., Yves-Alexandre De Montoye and Alex Pentland, Unique in the Shopping Mall: On the Reidentifiability of Credit Card Data, Science 347, no. 6221, pp. 536–539, January 30, 2015. <http://www.sciencemag.org/content/347/6221/536.abstract>; Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work, July 9, 2014. <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>; Mishari Almishari, Dali Kaafar, Gene Tsudik and Ekin Oguz, Are 140 Characters Enough? A Large-Scale Linkability Study of Tweets, 2014. <http://arxiv.org/pdf/1406.2746.pdf>; Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol. 57, pp. 1701–1777, 2010. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>; Arvind Narayanan and Vitaly Shmatikov, Robust De-Anonymization of Large Sparse Datasets, 2008. <http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>; Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Data Privacy Working Paper 3, 2000. <http://dataprivacylab.org/projects/identifiability/paper1.pdf>.

60 See, e.g., Paul M. Schwartz and Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, New York University Law Review, Vol. 86, pp. 1814–1894, 2011. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366>; Ohm (n. 59), p. 1701.

- *Notice and consent*: The traditional method of mitigating privacy concerns by providing notice to individuals about information privacy practices and obtaining consent is often thought to be ineffective, according to reports in the US,[61] EU,[62] and Switzerland[63]. Many studies suggest that consumers do not read highly complex, take-it-or-leave-it consent forms. If they did read them, it is not clear that they would understand the implications.[64] For instance, they may not realize that their consent to data gathering in one scenario could be used later for another purpose. The Internet of Things further punctuates this concern, as many sensors collect information about individuals before they have been notified or asked for consent.[65]
- *Accuracy of data and algorithmic accountability*: Data collected about and attributed to individuals is not always accurate, and it is difficult to correct even when inaccuracies are discovered. Additionally, the Big Data algorithms that are used to analyze personal data may not be transparent or understandable to individual subjects. Likewise, Internet of Things devices may have misinterpreted personal information, but recorded and processed

---

61 Executive Office of the President of the United States (n. 56), p. 40; U.S. Federal Trade Commission (FTC) (n. 56), p. 61.

62 Article 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, Adopted on December 1, 2009. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf>; European Union Agency for Network and Information Security (ENISA) (n. 57), p. 49.

63 The Swiss report on the evaluation of the Data Protection Act points out that Big Data and data mining systems are interested in collecting as much data as possible even if the purpose is not clear or only vaguely phrased. The report notes that the mechanisms of the Act fail to work when data is processed without transparency, i.e. when it is unclear that data is processed or who is processing data, or when data processing happens abroad. See Christian Bolliger, Marius Féraud, Astrid Epiney and Julia Haenni, Evaluation des Bundesgesetzes über den Datenschutz, Schlussbericht, March 10, 2011, p. 29. <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

64 See, e.g., Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia M. McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, Florian Schaub, Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding, Rochester, NY: Carnegie Mellon University, Center on Law and Information Policy at Fordham Law School, Center for Internet & Society, August 15, 2014. <http://papers.ssrn.com/abstract=2418297>.

65 See Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, Adopted September 16, 2014 («[...] In many cases, the user may not be aware of the data processing carried out by specific objects. Such lack of information constitutes a significant barrier to demonstrating valid consent under EU law [...]»). <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

it nonetheless. This opacity is cited as troubling in a number of US[66] and EU[67] privacy reports.

New or amplified privacy concerns

- *Predictive analytics*: Commentators in the US,[68] EU,[69] and Switzerland[70] alike are concerned with the emerging capability of Big Data predictive analytics, which – for instance – can be applied to evaluate an individual's propensity for criminal activity. Police can assemble lists of people with such «propensities» and subject them to enhanced law enforcement activities. Consequently, individuals will be pressured to avoid behavior that might be perceived as indicative of criminal tendencies. This concern can be generalized to any activity.
- *Discrimination and profiling*: There is a concern, primarily in US privacy reports, that Big Data predictive analytics will yield recommendations and insights that lead to discriminatory effects[71] and might even violate established antidiscrimination norms and laws.[72] The compilation of data points (that, by themselves, are not sensitive) into profiles that are used for automated decision making and discrimination of individuals is also addressed in reports from Switzerland[73] and the Council of Europe.[74]
- *Persistence of data and future uncertainty*: Since retaining vast amounts of data may be cheaper now than simply deleting it, the permanence of personal data[75] means that at some point in the future this data could be used for unanticipated purposes. For instance, data collected by an Internet of Things device could later be used for Big Data analytics in the life insurance industry. The current legal approach operates on the principle that a consumer is

---

66 Executive Office of the President of the United States (n. 56), p. 2; U.S. White House (n. 56), pp. 45–47; U.S. Federal Trade Commission (FTC) (n. 56), pp. 29–30.

67 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 10; Article 29 Data Protection Working Party/Working Party on Police and Justice (n. 62), p. 20.

68 U.S. White House (n. 56), p. 31.

69 Article 29 Data Protection Working Party (n. 65), p. 8.

70 See, e.g., Florent Thouvenin, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Rolf H. Weber and Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, pp. 61–83.

71 See, e.g., National Consumer Law Center, Big Data: A big Disappointment for Scoring Consumer Credit Risk, 2014. <http://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

72 Executive Office of the President of the United States (n. 56), p. 4; U.S. White House (n. 56), pp. 51–53.

73 Bolliger/Féraud/Epiney/Haenni (n. 63), p. 23.

74 Marc Dinant, Cécile de Terwangne and Jean-Philippe Moiny, Rapport Sur les Lacunes de la Convention N° 108 Pour la Protection des Personnes à L'égard du Traitement Automatisé des Données À Caractère Personnel Face aux Développements Technologiques, Council of Europe, 2010. <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD-BUR_2010_09%20FINAL.pdf>.

75 On the permanence of personal data, see generally Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton 2009.

given notice of collection and must provide consent for specific, limited uses.[76] However, this approach is in tension with the trend towards storing more data for unanticipated uses in the future; and, as noted above, the notice and consent model is often criticized for being ineffective in these circumstances. Privacy reports in the US[77] and the EU[78] highlight this concern and emphasize that such data should be kept secure, at a minimum, if not purposefully destroyed in a timely manner.

Cumulative effects

- *Loss of control*: Closely associated with the breakdown of the traditional notice and consent model, and as a cumulative effect of the all of the above-mentioned trends is the overarching concern shared across the US,[79] the EU,[80] and Switzerland[81] that users are losing the fundamental ability to control the flow of personal information. Similarly, privacy preferences, privacy settings, and other control mechanisms that were available to users in the past are no longer typical features of Big Data and Internet of Things applications.
- *Lack of public trust and consumer confidence*: Consumers generally expect that they will be notified and given the opportunity to consent to the collection and use of their information, and that their information will be used in the context in which it was provided. They bristle in response to privacy encroachments that are unexpected, especially if they consider them to have a «creepy» quality, as in the case of Target's models for predicting which of its customers were pregnant.[82] Meanwhile, perceived privacy and security risks may retard the adoption of socially useful Big Data processing techniques and Internet of Things devices, a concern underpinning reports in the US,[83] EU,[84] and other countries.

---

76 See, e.g., Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, Adopted on April 2, 2013. <http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf>.

77 U.S. White House (n. 56), pp. 53–54; U.S. Federal Trade Commission (FTC) (n. 56), p. 14–16.

78 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 50.

79 U.S. White House (n. 56), pp. 8–9; U.S. Federal Trade Commission (FTC) (n. 56), p. 9.

80 Article 29 Data Protection Working Party (n. 69), p. 6.

81 Hanspeter Thür, Zum Reformbedarf des Datenschutzgesetzes aus Sicht des Eidgenössischen Datenschutzbeauftragten, in: Astrid Epiney and Tobias Fasnacht (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes – Und Implikationen für die Schweiz, pp. 87–99, Zürich 2012.

82 Omar Tene and Jules Polonetsky, A Theory of Creepy: Technology, Privacy and Shifting Social Norms, 16 Yale J. L. & Tech, pp. 59–102, 2013. <http://pacscenter.stanford.edu/sites/all/files/Theory_of_Creepy_1.pdf >.

83 U.S. Federal Trade Commission (FTC) (n. 56), p. 18; U.S. White House (n. 56), p. 23.

84 European Union Agency for Network and Information Security (ENISA) (n. 57), pp. 1–2; Article 29 Data Protection Working Party (n. 65), pp. 3–4.

This brief survey suggests a broad *spectrum of privacy and privacy-related challenges and concerns* related to the phenomena of Big Data and the Internet of Things, ranging from questions about the effectiveness of traditional means and mechanisms aimed at protecting privacy on one end, to novel issues related to things such as predictive analytics and possible discriminatory effects on the other end – in addition to larger questions of trust. While some of the issues presented by these phenomena are novel, the two use cases are indicative of a typical pattern that emerges when innovative technologies meet the legal system,[85] including issues related to terminology and existing categories in addition to (at least in the case of radical innovations) qualitatively new questions and concerns.[86]

The overview of concerns also indicates that privacy is an important, but not exhaustive, dimension when considering the effects of Big Data and the Internet of Things on individuals and society at large. Such broader issues include, for instance, questions about *personal autonomy* (in the form of the freedom to make decisions based on options or offers that have not been pre-calculated or extrapolated from patterns discerned by algorithms) or concerns about *manipulation*[87] and *«filter bubbles.»*[88] Similarly, the enormous promise and potential benefits of the use cases highlight the need to put privacy considerations into a larger perspective – and ultimately balance privacy concerns against other values and interests.

B. Analyzing the Forces at Play

As the previous section demonstrates, the digital privacy crisis has not emerged in a vacuum. Rather, it has to be understood as the product of a *complex interplay* among a series of factors, which range from technical to human and economic to legal. It is impossible to provide a comprehensive analysis of all the relevant factors in the context of this report. However, the following paragraphs highlight a number of *key drivers* behind the larger ecosystem shifts as indi-

---

85 Urs Gasser, Cloud Innovation and the Law: Issues, Approaches, and Interplay, Berkman Center Research Publication No. 2014–7, March 17, 2014. <http://papers.ssrn.com/abstract=2410271>.

86 See, e.g., Urs Gasser and Herbert Burkert, Regulating Technological Innovation: An Information and a Business Law Perspective, in: Rechtliche Rahmenbedingungen des Wirtschaftsstandortes Schweiz: Festschrift 25 Jahre Juristische Abschlüsse an der Universität St. Gallen (HSG), pp. 503–523, Zürich, 2007.

87 Adam D. I. Kramer, Jamie E. Guillory and Jeffrey T. Hancock, Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks, 111 Proceedings of the National Academy of Sciences, pp. 8788–8790, June 17, 2014. <http://www.pnas.org/content/111/24/8788.full>.

88 Eli Pariser, The Filter Bubble: How the New Personalized Web Is Changing what We Read and How We Think, New York 2011.

cated by the Big Data phenomenon and the Internet of Things discussed in the previous section. From such a phenomenological perspective, four clusters of issues are particularly relevant: (1) technological drivers that include both «hardware» and «software»; (2) economic factors both in terms of larger macroeconomic trends and business model developments; (3) behavioral or «human» factors; and (4) various legal and policy decisions, which – perhaps counter-intuitively – have also contributed to the emergence of the digital privacy crisis.

I. Technological Factors

Fifteen years ago, the technologies that underlie new concepts like Big Data and the Internet of Things would not have been viable. The physical, data, and logical layers were not capable of providing the services necessary to support this data-rich ecosystem, at least not at scale, as the following points illustrate.

1. Physical Layer

The physical layer of infrastructure and hardware has become smaller, faster, more efficient, and capable of storing and transmitting large volumes of data for relatively low costs. Developments regarding microprocessors and storage media are illustrative of the massive transformations at the physical layer over the past decade:

- *Microprocessors* have improved exponentially at a constant cost. Intel's founder, Gordon Moore, famously observed in the 1960s and 1970s that the number of transistors – often used as an approximation for processing power – that could be manufactured onto a microprocessor would double every one to two years.[89] Coupled with other advances in microarchitecture, today's processors continue to make gains at smaller rates of change,[90] are substantially more powerful, and are capable of being packed into smaller, low-power devices.
- *Storage media* has undergone a similar evolution. When first introduced in the 1950s, the hard drive was «as big as two refrigerators» and provided five megabytes of storage for a purchase price of US $ 160,000 (or US $ 32,000 per megabyte).[91] Today, a desktop hard drive that stores six million megabytes can be purchased for less than US $ 300 (US $ 0.00005 per mega-

89 Gordon E. Moore, Cramming More Components onto Integrated Circuits, Electronics, pp. 114–117, April 19, 1965. <http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf>.

90 The End of Moore's Law, The Economist, April 19, 2015. <http://www.economist.com/blogs/economist-explains/2015/04/economist-explains-17>.

91 Prices adjusted for inflation. Rex Farrance, Timeline: 50 years of Hard Drives, PCWorld, September 16, 2006. <http://www.pcworld.com/article/127105/article.html>.

byte), with even larger capacities and lower prices on the horizon.[92] The consequence of these trends is that high-capacity storage media is now abundantly available and can be utilized on increasingly smaller-sized, portable devices.[93]

In addition to computing hardware, the *networking infrastructure* that allows for the transmission of data has become more robust. Networks are able to shuttle large amounts of bits along at increasingly faster speeds between wired and wireless devices. Internet access has generally become more ubiquitous and cheaper over time, and connections are available at homes, businesses, and in public places.[94] Meanwhile, an ever-increasing number of devices and sensors have networking functionality – ranging from televisions, video and still-image cameras, scales, thermostats, and the like.[95] *Networked devices* generate and capture data through sensors and often have the ability to share it with other devices.[96] These sensors are capable of detecting minute environmental changes, such as biometrics, location, and sounds that can assemble a detailed data profile.

2. *Data Layer*

As the technological and economic barriers to storage capacity lessen, it becomes possible for larger quantities of more precise information to be captured. Big Data and the Internet of Things are at the same time enabled by and contribute to a series of developments within the data layer, including exponential growth in the amount of data created and the collection of data from an increasing variety of sources – specifically:

- *Amount of data*: Individuals are increasingly generating information actively, as information is shared voluntarily and passively, as a by-product of interactions with computers.[97] According to IDC, the digital universe «is

92 Sebastian Anthony, Seagate Starts Shipping 8TB Hard Drives, with 10TB and HAMR on the Horizon, Extreme Tech, July 21, 2014. <http://www.extremetech.com/computing/186624-seagate-starts-shipping-8tb-hard-drives-with-10tb-and-hamr-on-the-horizon>.

93 John F. Gantz, The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010. IDC White Paper, March 2007. <https://www.emc.com/collateral/analyst-reports/expanding-digital-idc-white-paper.pdf>.

94 See, e.g., Berkman Center for Internet & Society at Harvard University, Next Generation Connectivity: A Review of Broadband Internet Transitions and Policy from Around the World, February 2010. <http://cyber.law.harvard.edu/pubrelease/broadband/>.

95 See, e.g., OECD (n. 35), Chapter 5: Emerging Issues.

96 The iPhone 6, for example, has two image sensors (i.e., cameras), a 3-axis gyroscope, a 3-axis accelerometer, a magnetometer, a proximity sensor, a barometer, an ambient light sensor, and a fingerprint reader, all of these in addition to a multitude of wireless capabilities. Apple, Inc., iPhone 6 Technology. <https://www.apple.com/iphone-6/technology/>.

97 See, e.g., Bruce Schneier, Data and Goliath, Norton: New York 2015, pp. 13–19; On the drivers of user-created content, see, e.g., OECD, Participative Web: User-Created Content, OECD Working Party on the Information Economy, April 12, 2007. <http://www.oecd.org/sti/38393115.pdf>.

growing by 40% a year into the next decade,» and it projects in 2020 the data generated worldwide will surpass 44 trillion gigabytes per year.[98] IDC also estimates that by this time «33% of the digital universe will contain information that might be valuable if analyzed.»[99] Businesses, as discussed in a later section, are incentivized to capture this information for its economic value. In addition, data-creating sensors are becoming common in public and private spaces. For instance, sensors can precisely track individuals in confined spaces, like public parks[100] or stores.[101]

- *Sources of data*: The sources of information vary greatly and include public sources such as social media and other web 2.0 websites in which individuals share information, from where data can be extracted using automated tools and application programming interfaces (APIs), or digitized public records. Other sources of information are proprietary or not visible to the public at large, including information derived from operating systems, software applications, mobile networks and Internet service providers, and networked devices. For instance, investigations of popular smartphone applications have revealed that many apps are passively collecting and transmitting data, including age, gender, and other personal information, to third parties.[102]

Not only have the amount and sources of data multiplied, but also the *granularity* of the information collected has changed, as the example of data collected and inferred from tracking users on Internet websites illustrates. A frequently cited investigative report, for instance, found that each of the top 50 US websites «on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning.»[103] Such *tracking tools* have become more sophisticated, persistently tracking users across browsing sessions and scanning «in real time what people are doing on a web page, then instantly assessing location, income, shopping interests and even medical conditions.»[104]

---

98 IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, April 2014. <http://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm>.

99 John Gantz and David Reinsel, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, IDC, December 2012. <http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf>.

100 See, e.g., David Heinzmann, New Sensors Will Scoop Up Big Data' on Chicago, Chicago Tribune, June 20, 2014. <http://articles.chicagotribune.com/2014-06-20/news/ct-big-data-chicago-20140621_1_cell-phone-data-big-data-sensors>; Stacey Kuznetsov and Eric Paulos, Participatory Sensing in Public Spaces: Activating Urban Surfaces with Sensor Probes, Proceedings of the 8th ACM Conference on Designing Interactive Systems, pp. 21–30, August 2010. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.167.5517&rep=rep1&type=pdf>.

101 Clifford (n. 30).

102 Scott Thrum and Yukari Iwatani Kane, Your Apps Are Watching You, Wall Street Journal, December 18, 2010. <http://www.wsj.com/articles/SB10001424052748704368004576027751867039730>.

103 Julia Angwin, The Web's New Gold Mine: Your Secrets, Wall Street Journal, July 30, 2010. <http://www.wsj.com/articles/SB10001424052748703940904575395073512989404>.

104 Angwin (n. 103).

3. *Logical Layer*

As the size, variety, and granularity of data has grown exponentially, improved *platforms* and frameworks to manage and analyze large data sets have emerged. For instance, Apache's Hadoop, an open source data-processing platform, has been regarded as a key development in the Big Data analytics space.[105] Hadoop enables the processing and analysis of very large, distributed datasets in a flexible manner that allows companies to quickly scale tools for analyzing data.[106] Unlike traditional databases, data in Hadoop does not need to adhere to a schema or be overly structured, which allows for the data to be bigger and «messier» with less overhead required for managing it. By deploying Hadoop in cloud computing environments, companies can manage and analyze more data for less cost.

The *analytics tools* being used to analyze data are becoming more precise and have more applications. Companies like SAP, Vertica, and ParAccel have developed new tools which – among other things – include significant parallel processing capabilities, in-memory databases, and columnar features which allow companies to handle and analyze data in ways not previously possible.[107] Additionally, existing analytics tools have been updated and improved. For example, in addition to recent improvements to Hadoop that will allow for enhanced data provisioning and scaling,[108] IBM, Hortonworks, and EMC Pivotal have announced measures to insure the interoperability of their Hadoop-based platforms for improved processing.[109] Data mining techniques can identify patterns and relationships between pieces of information in large data sets, and machine learning can also be used to extract predictive models from data. For example, algorithms have become increasingly adept at identifying anomalies in credit card purchases that might indicate fraud,[110] recognizing and interpreting human speech, and predicting relationships between people.[111] Recently, Ama-

---

105 See, e.g., Doug Henschen, 16 Top Big Data Analytics Platforms, Information Week, January 30, 2014. <http://www.informationweek.com/big-data/big-data-analytics/16-top-big-data-analytics-platforms/d/d-id/1113609>.

106 Brian Proffitt, Hadoop: What It Is and How It Works, ReadWrite, May 23, 2013. <http://readwrite.com/2013/05/23/hadoop-what-it-is-and-how-it-works>.

107 Jaikumar Vijayan, New Tools Driving Big Data Analytics, Survey Finds, Computerworld, August 25, 2011. <http://www.computerworld.com/article/2510790/business-intelligence/new-tools-driving-big-data-analytics–survey-finds.html>.

108 James Nunns, Hortonworks Drops a Trunkfull of Hadoop Upgrades, Computer Business Review, April 15, 2015. <http://www.cbronline.com/news/enterprise-it/software/hortonworks-drops-a-trunkful-of-hadoop-upgrades-4554696>.

109 Chris Preimesberger, HortonWorks, IBM, Pivotal Align Hadoop Platforms on ODP Core, eWeek, April 16, 2015. <http://www.eweek.com/enterprise-apps/hortonworks-ibm-pivotal-align-hadoop-platforms-on-odp-core.html>.

110 John Akhilomen, Data Mining Application for Cyber Credit-Card Fraud Detection System, Proceedings of the World Conference on Engineering 2014, London, Vol. 3, 2013. <http://www.iaeng.org/publication/WCE2013/WCE2013_pp1537–1542.pdf>.

111 Robert D. Hof, Deep Learning, MIT Technology Review, April 23, 2013. <http://www.technologyreview.com/featuredstory/513696/deep-learning>.

zon launched a machine learning feature for web services that allows individuals and companies to utilize Amazon's learning systems to make predictions, a development which might have significant implications both for small firms who could not afford to build such capabilities on their own and – by extension – users, who will benefit from increased accuracy in the predictive power of apps and websites in areas such as personalized product recommendations.[112]

II. Economic Factors

Whether looking at the macro-level and considering the larger shift towards an economy that is increasingly based on and fueled by data,[113] or zooming in on the micro-level of individual companies and other participants in the digital economy,[114] economic factors are key in understanding the origins, speed, and future trajectories of the shifts that form the undercurrents of the digital privacy crisis outlined.

1. Supply- and Demand-Side Drivers

Economic enablers and drivers of the fundamental changes in the global economy have been analyzed and tracked over recent years in various reports and cover a broad range of industries, sectors, and actors, from Internet-related services and hardware to telecommunication and software services.[115] The supply- and demand-side factors that drive the Big Data and Internet of Things economies illustrate both the scale and dynamics at play:

- On the *supply side*, investments in the Big Data and Internet of Things industry are very strong and the outlook, according to analysts, forecasts industry growth.[116] Estimates by McKinsey Global Institute indicate that, in seven key industries, Big Data could generate an additional US $ 3 trillion globally in value every year, US $ 1.3 trillion of which would benefit the United States.[117] Similarly, Gartner estimates that the worldwide Internet of

112 Jon Fingas, Amazon's Web Services Are Smart Enough to Make Predictions, Engadget, April 11, 2015. <http://www.engadget.com/2015/04/11/amazon-machine-learning/>.

113 See, e.g., OECD, Measuring the Digital Economy: A New Perspective, December 2014. <http://www.oecd.org/sti/measuring-the-digital-economy-9789264221796-en.htm>: Du Rausas/Manyika/Hazen/Bughin/Chui/Said, (n. 11).

114 See, e.g., OECD (n. 113), pp. 128–149.

115 See, e.g., OECD (n. 113), pp. 25–47.

116 Louis Columbus, 2014: The Year Big Data Adoption Goes Mainstream in the Enterprise, Forbes, January 12, 2014. <http://www.forbes.com/sites/louiscolumbus/2014/01/12/2014-the-year-big-data-adoption-goes-mainstream-in-the-enterprise/>.

117 James Manyika, Michael Chui, Diana Farrell, Steve Van Kuiken, Peter Groves and Elizabeth Almasi Doshi, Open Data: Unlocking Innovation and Performance with Liquid Information, McKinsey & Company, October 2013. <http://www.mckinsey.com/insights/busi

Things will support services spending of US $ 69.5 billion in 2015, and more than US $ 263 billion by 2020.[118]

- On the *demand side*, a growing number of businesses from all sectors are using data analytics to gain new insights into operating environments, better allocate resources, target relevant advertising, improve human decision making, and apply machine-learning approaches to automate decision making by computers. For both ICT and non-ICT firms, studies indicate that the use of data and analytics results in a 5-10 % increase in productivity,[119] and surveys suggest performance increases of up to 40 % – indicators of both the value placed on Big Data and the demand for data by firms. Internet of Things consumer and enterprise devices are already in high demand, and sales are predicted to grow strongly over the coming years. IDC estimates that by 2020, the market will be US $ 7.1 trillion worldwide.[120]

The falling costs and rapid technological improvements discussed above have played a key role in the speed at which this industry niche has taken shape. Likewise, the availability of cloud computing infrastructure has enabled companies to quickly scale their infrastructure capabilities to meet demand without costly capital investments that would otherwise be a financial barrier. This means that more companies, whether well-established multinational corporations or small startups, can potentially participate in the data industry.

2. *Business Model Evolution*

In addition to the transformations driven by the larger economic trends mentioned above, new generations of business models that rely heavily on data about users are an important factor when analyzing the digital privacy crisis and situating it in its relevant context. Two related developments are particularly noteworthy:

- *Ad-based business models*: Since the 1990s, online advertising has become a primary source of revenue for many Internet companies.[121] More specifically, advertising has been used to subsidize free web content and services – such as webmail, blogs, and news media – while moving away from models based on subscription fees. The Interactive Advertising Bureau in Europe,

---

ness_technology/open_data_unlocking_innovation_and_performance_with_liquid_information>.

118 Gartner Says 4.9 Billion Connected ‹Things' Will be in Use in 2015, Gartner, November 11, 2014. <http://www.gartner.com/newsroom/id/2905717>.

119 OECD, Data-Driven Innovation for Growth and Well-Being, Interim Synthesis Report, October 2014, p. 5. <http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf>.

120 Leon Spencer, Internet of Things market to hit $ 7.1 trillion by 2020: IDC, ZD Net, June 5, 2014. <http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/>.

121 Catherine Tucker, The Economics Value of Online Customer Data, OECD: 30 Years After the OECD Privacy Guidelines Workshop, December 1, 2010. <http://www.oecd.org/sti/ieconomy/46968839.pdf>.

for instance, concludes that much of today's content and many services and applications available on the Internet are supplied at no cost to the consumer thanks to this model.[122]

- *Targeted advertisement*: The technologies that Google and Facebook use to target specific individuals based on detailed information about their online and offline activities first emerged towards the later half of the 1990 s.[123] This widespread practice is often described as online behavioral advertising. While other revenue models – including the «freemium» approach, a hybrid of free and subscription services – have emerged and continue to evolve, advertising-supported business models are currently dominant in the US and Europe.[124]

There are several reasons why this advertising model has become so entrenched. For instance, online advertising in general is more measurable than traditional forms of advertising, which means advertisers can track the effectiveness and conversion ratio of their marketing campaigns.[125] Behavioral advertising is also believed to be more effective than other forms of Internet advertising because it is more tailored to interests, such as contextual advertising and display advertising, and therefore often valued higher by advertisers.[126] Finally, consumers have become accustomed to freely available content, services, and applications, which is not possible without a reliable source of revenue.[127]

Together, these reasons help explain why so many Internet companies are collecting data: there exists a clear path to *monetizing* it through data-driven advertising and information resale. As a result, a rich marketplace for purchasing and selling data and accessing users for online advertising purposes has emerged.[128] This marketplace includes a range of third-party actors, including

---

122 Interactive Advertising Bureau Europe, Advertising on the Internet: A Quick Download for Policy Makers, A Briefing by IAB Europe. <http://www.iab.fi/media/pdf-tiedostot/iab-europen-verkkomainonnan-opas-advertising-on-the-internet.pdf>.

123 See David S. Evans, The Online Advertising Industry: Economics, Evolution, and Privacy, Journal of Economic Perspectives, Vol. 23, Number 3, pp. 37–60, 2009. <http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.23.3.37>.

124 Interactive Advertising Bureau Europe (n. 122); Avi Goldfarb and Victor J. Tremblay, Introduction: The Economics of Internet Advertising, Review of Industrial Organization, Vol. 44, No. 2, August 13, pp. 113–14, 2013.

125 Tucker (n. 121), p. 16.

126 See, e.g., Catherine Tucker, The Economics of Advertising and Privacy, November 19, 2011. <http://cetucker.scripts.mit.edu/docs/econ_summary_2011.pdf>; Behavioral Targeting Brings Clear Benefits to Publishers: But how Clear are the Advantages to Consumers?, EMarketer, August 23, 2010. <http://www.emarketer.com/Article/Behavioral-Targeting-Brings-Clear-Benefits-Publishers/1007884>.

127 Interactive Advertising Bureau Europe (n. 122).

128 See, e.g., U.S. Government Accountability Office, Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace, GAO-13-663, September 11, 2013. <http://www.gao.gov/assets/660/658151.pdf>.

information aggregators, brokers, and resellers as well as advertising networks, platforms, and exchanges.[129]

In addition, data collected from users is also utilized by Internet companies for purposes outside of direct advertising in ways that still relate to their business models.[130] For instance, data about individuals' usage habits can be used to provide companies with immediate feedback about a product, which is useful for making improvements and earning customer satisfaction. Data can also enable companies to offer more compelling or useful products, which may give them a competitive advantage over others.[131]

III. Behavioral Factors

In addition to technological advancements and economic enablers, the development and adoption of privacy-relevant digital technologies is in large part driven by *human factors*: the behavior and demand of users and their communities. As with the other drivers of the broader tectonic shifts that fuel changes in the digitally connected environment from which privacy challenges emerge, the human factors that need to be considered when seeking to gain a deeper understanding of the current state of affairs are multi-faceted and nuanced. For the purpose of this report, three aspects of the more complex human environment are particularly relevant: (1) consumer demand and broad adoption of digital technologies and services that involve the collection and processing of personal information; (2) the interplay between human and technological factors, especially technological design; and (3) what one might call «complicating human factors» that contribute to the digital privacy crisis and also have consequences for possible remedies, as discussed in later parts of this report.

1. Consumer Demand

While it is important to recognize that the digital divide and the participation (and skill) gap, respectively, are still a major area of concern and roadblock in the development of a participatory digital environment,[132] empirical data from

---

129 U.S. Interactive Advertising Bureau, Advertising Ecosystem. <http://www.iab.net/data/ecosystem.html>.

130 Tucker (n. 121), p. 18.

131 Tim McGuire, James Manyika and Michael Chui, Why Big Data Is the New Competitive Advantage, Ivey Business Journal, July/August 2012. <http://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/>.

132 For general statistics on the state of the global information society see, e.g., International Telecommunication Union, Measuring the Information Society, Geneva, 2013. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf>; and for a discussion of participation and skills gap, see, e.g., Eszter Hargittai and Gina Walejko, The Participation Divide: Content Creation and Sharing in the Digital Age, Information, Communication & Society, Vol. 11, No. 2, pp. 239–56, March 1, 2008.

the US and Europe demonstrates that the digital consumer technologies and services introduced in this report have been widely adopted by large parts of the population. Most recent surveys looking at the digital media usage habits of *young people* illustrate this overall trend.[133] According to the most recent US survey data, for instance, 24% of teens are almost constantly online, facilitated by the widespread availability of smartphones and other mobile devices, as nearly three-quarters of teens have or have access to a smartphone. A large majority of teens (71%) are using more than one social networking site, with Facebook, Instagram, and Snapchat the most used platforms among US teens.[134] Data from Switzerland, to take an example from Europe, paints a similar picture, with some nuances. According to the leading study in the field, 97% of Swiss youth age 12–19 own a smartphone and use the Internet heavily, including services that extensively collect and aggregate personal information, such as Facebook, which is used by 79% of Swiss teens daily or at least multiple times per week.[135]

These and related trends in the adoption of new devices and technologies reflect broad *social changes*. Digital devices and services are viewed as necessities for full participation in modern life.[136] As a large body of research suggests, the meaningful use of digital technology is not limited to young people or «Digital Natives»;[137] rather, many of the most essential social, professional, and civic activities are now at least partially conducted via Internet-connected devices, including social and business communications, news media and entertainment consumption, interactions with the government, and participation in political discourse.[138]

In particular, consumer demand drives the development of digital devices and services that offer gains in efficiency and convenience, and consumers are generally willing to exchange their personal information for free services offering these advantages. One way that services provide more relevant information is through analytics and personalization that leverage the personal information

---

133 For information on youth privacy perspectives and online behavior, see generally, Carrie James, Disconnected: Youth, New Media, and the Ethics Gaps, Cambridge 2014.

134 Amanda Lenhart, Teens, Social Media & Technology Overview 2015, Pew Research Center, April 9, 2015. <http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf>.

135 Isabel Willemse, Gregor Waller, Sarah Genner, Lilian Suter, Sabine Oppliger, Anna-Lena Huber and Daniel Suess, Jugend, Aktivitäten, Medien – Erhebung Schweiz, Zürich, ZHAW Zürcher Hochschule für Angewandte Wissenschaften. <http://www.zhaw.ch/fileadmin/user_upload/psychologie/Downloads/Forschung/JAMES/JAMES_2015/Ergebnisbericht_JAMES_2014.pdf>.

136 See, e.g., Ofcom, Results of Research into Consumer Views on the Importance of Communications Services and their Affordability: Report on Findings, July 22, 2014. <http://stakeholders.ofcom.org.uk/binaries/research/affordability/affordability_report.pdf>.

137 John Palfrey and Urs Gasser, Born Digital, New York 2008.

138 See, e.g., Lee Rainie and Barry Wellman, Networked: The New Social Operating System, Cambridge 2012.

generated through the use of the services. For instance, Amazon uses algorithms to target product advertisements to consumers based on their purchase history and the purchases of other consumers,[139] and Facebook curates a feed of relevant information for each user based on the user's activity on the service.[140]

2. *Interplay Between Design and Behavior*

Individual behavior and technological development are in an interactive relationship. The use of *interface design*, including techniques such as «charismatic code,»[141] aimed at nudging user behavior in particular directions has long been practiced in the digital media space, but also recognized in the scholarly literature, for instance in the context of peer-to-peer transactions and various forms of online cooperation.[142] With respect to digital privacy, the use of interface design and default settings by platform providers – such as social media services – to encourage users to «share» information and make it publicly available through default settings are particularly relevant.[143] Some social networks, for instance, encourage users to reveal personal details by prompting them to complete fields, as Facebook does with information related to location, date of birth, and relationship status.[144]

Conversely, user behavior and corresponding social norms (often themselves shaped by repeated interactions with interface designs) recursively impact product design. Case studies demonstrate and analyze how privacy-related options and defaults provided by online services are evolving over time, as developers experiment with different approaches and evaluate how individual behavior shifts in response.[145] As further discussed below in the market-based approaches section of

---

139 See, e.g., JP Mangalindan, Amazon's Recommendation Secret, Fortune, July 30, 2012. <http://www.fortune.com/2012/07/30/amazons-recommendation-secret>.

140 See, e.g., Mat Honan, I Liked Everything I Saw on Facebook. Here's What It Did to Me, Wired, August 11, 2014. <http://www.wired.com/2014/08/i-liked-everything-i-saw-on-facebook-for-two-days-heres-what-it-did-to-me>.

141 See, e.g., Lior Strahilevitz, Charismatic Code, Social Norms, and the Emergence of File-Sharing Networks, Virginia Law Review, Vol. 89, No. 3, pp. 505–595, 2003. <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1130&context=journal_articles>.

142 See, e.g., Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom, New Haven 2007; Yochai Benkler, The Penguin and the Leviathan: How Cooperation Triumphs over Self-Interest, New York 2011.

143 See, e.g., Twitter, Privacy Policy. <https://twitter.com/privacy?lang=en> («Any registered user can send a Tweet, which is a message of 140 characters or less that is public by default and can include other content like photos, videos, and links to other websites.»); Instagram, FAQ. <https://instagram.com/about/faq> («All photos are public by default which means they are visible to anyone using Instagram or on the instagram.com website.»).

144 See, e.g., Zachary M. Seward, The History of Facebook As Told Through Its Ever-Expanding List of Profile Fields, Quartz, March 7, 2013. <http://www.qz.com/60323/facebook-at-told-through-its-ever-expanding-list-of-profile-fields>.

145 Fred Stutzman, Ralph Gross and Alessandro Acquisti, Silent Listeners: The Evolution of Privacy and Disclosure on Facebook, Journal of Privacy and Confidentiality, Vol. 4, No. 2, pp. 7–41, 2012. <http://repository.cmu.edu/jpc/vol4/iss2/2>.

this report, anecdotal evidence suggests that there is a growing awareness among *developers* of the privacy-related expectations of users[146] as they increasingly demand greater privacy protections embedded within services,[147] especially in response to encroachments on privacy that are considered to have a «creepy» quality.[148]

Developers address these demands in various ways, for instance by encrypting all data in storage or transit by default.[149] Some social networks, to take another example, introduce privacy protections by making the content shared by users visible only to approved individuals by default or by prompting users periodically to choose privacy settings.[150] Organizational changes, such as the hiring of chief privacy officers and incorporating the principles of privacy by design into product development processes are other manifestations of privacy awareness, as discussed later in this report.

3. *Complicating Factors*

Certain aspects and characteristics of human behavior that interact with digital technology are complicating the picture when viewed through the lens of digital privacy and need to be taken into account when exploring possible responses to the current privacy crisis. Some of the particularities are discussed in greater detail in the section on human-centered approaches below, but it is worth highlighting three such complicating elements.

- *Incomplete and asymmetric information*: In order for consumers to decide how much information to share and to balance, for instance, the tradeoffs between the convenience of a service and the privacy risks associated with it, they must understand how and to what extent they are giving up their privacy. However, users typically do not have clear knowledge about the extent to which data is gathered and retained, analyzed to target advertising or for other purposes, combined with data from other sources, and disclosed to

146 For information on the privacy perceptions and preferences of European users, see Patil Sunil, Bhanu Patruni, Hui Lu, Fay Dunkerley, James Fox, Dimitris Potoglou and Neil Robinson, Public Perception of Security and Privacy: Results of the Comprehensive Analysis of PACT's Pan-European Survey, Rand Europe, 2015. <http://www.rand.org/pubs/research_reports/RR704.html>.

147 See, e.g., Marry Madden, Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research Center, November 12, 2014, pp. 37–38. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions>.

148 Tene/Polonetsky (n. 82).

149 See, e.g., Joe Miller, Google and Apple to Introduce Default Encryption, BBC.com News, September 19, 2014. <http://www.bbc.com/news/technology-29276955>.

150 See, e.g., Sanjay Kairam, Michael J. Brzozowski, David Huffaker and Ed H. Chi, Talking in Circles: Selective Sharing in Google+, Proceedings of the ACM Conference on Human Factors in Computing System, 1065–1074, 2012; Paddy Underwood, Privacy Checkup Is Now Rolling Out, Facebook Newsroom, September 4, 2014. <http://newsroom.fb.com/news/2014/09/privacy-checkup-is-now-rolling-out>.

third parties hidden from the public. The uncertainty is exacerbated by the difficulty of anticipating and understanding the potential consequences – including harms – of privacy behavior in the future, which is often intangible.[151]

- *Privacy paradox*: Many individuals claim to value their privacy very highly, while acting in ways that expose themselves to greater privacy risks. This discrepancy between privacy attitudes and behavior is referred to as the privacy paradox.[152] In a recent survey by the Pew Research Center, for instance, 43 % of Americans expressed that they are unwilling to share personal data in exchange for access to free online services, and 61 % said they did not value the greater efficiency of online services due to personal data collection.[153] But these stated preferences contradict actual user behavior with respect to digital services, such as social networking sites.[154]
- *Fluidity*: A third complicating factor when both identifying and seeking to address digital privacy challenges is the fluidity of user behavior. Again, the example of young Internet users is illustrative. For instance, a series of studies demonstrate that US teens recently started diversifying the social media platforms they use – in part motivated by privacy-relevant considerations such as audience and reputation management.[155] This platform diversification can be seen as a form of organic individual and social learning when dealing with privacy issues, which makes determining the appropriate timing of any potential (legal, design, etc.) intervention difficult to determine.[156]

The three complicating behavioral factors highlighted here – several others could be added – are illustrative of some of the larger *diagnostic and design*

---

151 See, e.g., Alessandro Acquisti, Laura Brandimarte and George Loewenstein, Privacy and Human Behavior in the Age of Information, Science, Vol. 347, No. 6221, pp. 509–514, January 30, 2015. <http://www.sciencemag.org/content/347/6221/509.full>.

152 See, e.g., Sarah Spiekermann, Jens Grossklags and Bettina Berendt, E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior, Third ACM Conference on Electronic Commerce, pp. 38–47, 2001. <http://www.ijsselsteijn.nl/slides/Spiekermann.pdf>; Susan B. Barnes, A Privacy Paradox: Social Networking in the United States, First Monday, Vol. 11, No. 9, September 4, 2006. <http://firstmonday.org/ojs/index.php/fm/article/view/1394>. See also Acquisti/Brandimarte/Loewenstein (n. 151), pp. 510–511.

153 Madden (n. 147), pp. 37–38.

154 See, e.g., Spiekermann/Grossklags/Berendt (n. 152), p. 45; Tobias Dienlin and Sabine Trepte, Putting the Social (Psychology) into Social Media, European Journal of Social Psychology, 2014. <http://www.readcube.com/articles/10.1002%2Fejsp.2049?r3_referer=wol&tracking_action=preview_click&show_checkout=1&purchase_referrer=onlinelibrary.wiley.com&purchase_site_license=LICENSE_DENIED_NO_CUSTOMER>.

155 See, e.g., Lenhart (n. 134); Sandra Cortesi, Youth Online: Diversifying Social Media Platforms and Practices, in: Urs Gasser, Robert Faris, and Rebekah Heacock Jones (eds.), Internet Monitor 2013: Reflections on the Digital World, Berkman Research Publication Series No. 2013–27. <http://papers.ssrn.com/abstract=2366840>.

156 See, e.g., Urs Gasser, Youth and Digital Media Research and Policy-Making Interface: Mapping Key Design Challenges, in: Sandra Cortesi and Urs Gasser (eds.), Digitally Connected: Global Perspectives on Youth and Digital Media, Berkman Research Publication Series No. 2015–6. <http://papers.ssrn.com/abstract=2585686>.

challenges when managing the digital privacy crisis, which is not only characterized by high degrees of technical complexity and special economic conditions in the underlying markets (such as strong network effects) but also by a great deal of uncertainty and fluidity when it comes to human behavior that interacts with the digital ecosystem.

IV. Legal Factors

The technical, economic, and behavioral forces outlined in the previous paragraphs interact in manifold ways with legal factors. Indeed, the emergence and evolution of the digitally networked environment has been deeply affected by a long series of typically decentralized – and at times implicit – *choices by law- and policymakers*, as well as *regulators* across many domains and levels of the legal and larger institutional system.[157] Viewed from such an ecosystem perspective, the law has played a vital role in the development and adoption of digital technology, as well as the commercial and government use of data and digital services. In order to gain a deeper understanding of the interplay between the legal system and the digital ecosystem generally – and digital privacy in particular – it is helpful to differentiate among three basic functions the law can serve: the role of a constraint, enabler, or leveler.

1. Law as Constraint, Enabler, or Leveler[158]

In the context of digital technology, law has been traditionally framed as a *constraint* on behavior.[159] Legal norms that impose ex post liability for certain behaviors are examples of law functioning as a constraint. Such a (restrictive) understanding of law has shaped the notion of «code as law,» where software constrains user behavior ex ante, as embedded in hardware or software – a concept that will be further addressed below when examining technology-based approaches to the digital privacy crisis.[160]

However, law can also serve the role of an *enabler*, where it opens up spaces for technological and social innovation and interaction, enables transactions, and supports various modes of production and collaboration. Contract law is an example of enabling law, as it allows innovators to privately stipulate the «ground rules» of transactions. To name two other innovation-relevant examples, intellectual property and trade laws provide incentives to innovate via baseline legal protections.

---

157 Illustrative the role law has played with respect to the emergence of the Internet itself, see Vanessa Geczy-Sparwasser, Die Gesetzgebungsgeschichte des Internet, Berlin 2003.

158 This subsection is based on Gasser (n. 85).

159 See, e.g. Lawrence Lessig, The New Chicago School, Journal of Legal Studies, Vol. 27, June 1998.

160 Lessig (n. 13).

The third basic function of law in the context of innovation is as a *leveler*. In this function, the law aims to correct a normative or market imbalance in power. Competition law aimed at protecting consumer welfare, model contract laws aimed at reducing asymmetries between contracting parties, or legal approaches in support of standard-setting in the technical field are situations where the legal system serves a leveling function in the Internet age.

2. *Example: Cloud Computing*

Cloud computing – as mentioned before – serves as a key enabling platform for Big Data applications and services, as well as a *foundational technology* for the Internet of Things.[161] It is a particularly interesting case study that illustrates the different functions of law at the level of technological architecture and across different legal and regulatory domains, and how it shapes the development of the digitally networked environment.[162]

- *Enabler*: The availability of contract law and corresponding enforcement mechanisms, for instance, is key for creating a viable transactional environment where cloud providers and users can engage in privately ordering. Licensing arrangements enable the transfer of intellectual assets and knowledge between cloud computing developers.
- *Leveler*: In the EU, the proposed Regulation on a Common European Sales Law aims to foster cross-jurisdictional transactions in the cloud age and is an example of law's leveling powers.[163] Governmental support of standard-setting initiatives, such as the National Institute for Standards and Technology (NIST) in the US, both enables an interoperable marketplace and levels imbalances created by proprietary standards.[164]
- *Constraint*: Several recently proposed laws are aimed at constraining the behavior of cloud providers with respect to the collection, processing, and use of personal information.[165] Similarly, soft laws in the form of standards

---

161 See, e.g., Palfrey/Gasser (n. 10), Chapter 13: Architectures of the Future; see also Christopher Millard (ed.), Cloud Computing Law, Oxford 2013.

162 See for a detailed analysis Urs Gasser and David O'Brien, Governments and Cloud Computing: Roles, Approaches, and Policy Considerations, Berkman Center Research Publication Series No. 2014-6, March 17, 2014. <http://papers.ssrn.com/abstract=2410270>.

163 European Commission, Regulation of the European Parliament and of the Council on a Common European Sales Law, Brussels, October 11, 2011. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0635:FIN:en:PDF>.

164 Cloud Computing Program. <http://www.nist.gov/itl/cloud/>.

165 In the US, see, e.g., H.R. 5777, 111th Cong. 2d Sess., July 19, 2010. <http://www.gpo.gov/fdsys/pkg/BILLS-111hr5777ih/pdf/BILLS-111hr5777ih.pdf>; in the EU see, e.g., European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, Brussels, 25.1.2012, COM(2011) 11 final. <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.

aimed at protecting data privacy and security in the cloud contain constraining elements.[166]

The example of cloud computing illustrates how the legal system interacts in multiple ways with the digital environment and shapes the development and use of digital technologies. These interactions at the system level also have at least *indirect* downstream ramifications for digital privacy.[167] However, as the next section illustrates, the different functions of law do not only play out at the meta-level of interconnected systems;[168] they can also be observed when looking at privacy and digital privacy law as one specific regulatory domain, when legislators attempt to protect individual privacy interests and enforce social norms of privacy while remaining flexible to adapt to new technologies and industries.

3. *Example: US Privacy Law*

Within a particular privacy regime of a given jurisdiction – taking the US as one possible example in this paragraph – one can identify the above-mentioned three basic functions of law. For instance, the obligations and safeguards that apply to covered entities under sector-specific privacy laws restrict what these actors can legally do with personal information, thus serving a constraining function. Mechanisms such as the consent principle or exemptions are examples where the same body of law serves an enabling function with respect to data collection and usage. Information obligations vis-à-vis the data subject, for instance, illustrate where law plays the role of a leveler by reducing information asymmetries and aiming to create a more level playing field.[169]

For complex historical, cultural, and other contextual reasons (including the play of the larger political economy)[170] and varying public policy goals, law and policymakers in different countries have made different choices over time with respect to the exact mix of constraining, enabling, and leveling functions of norms aimed at regulating digital technology generally and data in particular.[171] Of particular interest in the thematic context of this report is the United

---

166 Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors, ISO, 2014. <http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498>.

167 See, e.g., Gasser/O'Brien (n. 162).

168 See, e.g., Palfrey/Gasser (n. 10).

169 See, e.g., Handbook on European Data Protection Law, Council of Europe – European Union Agency for Fundamental Rights, Luxembourg 2014. <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>.

170 See, e.g., Powers/Jablonski (n. 12).

171 See, e.g., Daniel J. Solove, A Brief History of Information Privacy Law, GWU Law School Public Law Research Paper No. 215, July 10, 2006. <http://papers.ssrn.com/abstract=914271>; Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Ithaca 1992; Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill 2009.

States, which leads the global Internet supply ecosystem by capturing more than 30% of global Internet revenues and more than 40% of net income.[172] In the US, legislators have adopted privacy statutes that regulate a limited set of industry sectors,[173] but have largely decided to leave the market to *self-regulate*. President Clinton was a strong proponent of self-regulation of electronic commerce beginning in 1997,[174] and the Federal Trade Commission (FTC) has supported self-regulation of fair information practices since 1998.[175]

Critics have identified many advantages and disadvantages to this approach, as further discussed later in this report. On one hand, self-regulation is viewed by many to be more effective, efficient, and flexible than the law because industry is best equipped to predict the privacy-related challenges, to allocate resources to the most pressing problems, and standards developed by industry are less likely to be resisted by industry.[176] As industry observers have argued, the lack of a comprehensive privacy law and the reliance on notice and consent, self-regulation, and codes of conduct have contributed to the exponential growth in personal data-driven technologies.[177] On the other hand, others are concerned that self-regulatory standards are too weak, that they weigh too heavily in favor of business models and against individual privacy interests, lack transparency, and that self-regulatory standards are less likely to be enforced than government standards.[178]

---

172 Du Rausas/Manyika/Hazen/Bughin/Chui/Said (n. 11).

173 US privacy statutes make guarantees to individuals that the personal information from their medical (Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E.), financial (Fair Credit Reporting Act, Pub. L. 91–508, 84 Stat. 1114; Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338), and educational records (Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, 34 C.F.R. Part 99), will be safeguarded and disclosed only for limited purposes. Laws also protect individuals from discrimination based on the usage of certain types of personal information (Genetic Information Nondiscrimination Act of 2008, Pub. L. 110–233, 122 Stat. 881) to alleviate concerns about the misuse of sensitive personal information and to enable individuals to freely seek medical care, financial services, and education and training. The US Federal Trade Commission (FTC) similarly protects the privacy interests of consumers by investigating and preventing commercial firms from engaging in unfair and deceptive practices (Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45). For an overview, see, e.g., Daniel J. Solove and Paul Schwartz, Information Privacy Law, Fourth Edition, New York 2011.

174 U.S. White House, Presidential Directive on E-Commerce, July 1, 1997. <http://fas.org/irp/offdocs/pdd-nec-ec.htm>.

175 U.S. Federal Trade Commission (FTC), Privacy Online: A Report to Congress, June 1998. <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

176 See generally Rolf H. Weber, Towards a Legal Framework for the Information Society, Zurich 2003, pp. 72–73.

177 See, e.g., Natasha Singer, Data Protection Laws, an Ocean Apart, The New York Times, February 3, 2013.

178 See, e.g., Chris Jay Hoofnagle, Privacy Self Regulation: A Decade of Disappointment in: Jane K. Winn (ed.), Consumer Protection in the Age of the ‹Information Economy›, pp. 379–402, Hampshire and Burlington 2006.

While the discussion about the merits and drawbacks of the US approach to privacy continues, the legal and regulatory landscape is gradually evolving in response to the technological, economic, and normative developments outlined above. The viability of the traditional regulatory model of notice and consent relies on the assumption that individuals can make well-reasoned decisions about sharing their personal information. Yet, as discussed above, factors such as information asymmetry and uncertainty regarding privacy preferences (other limitations such as bounded rationality are further discussed below) make it increasingly difficult for individuals to reason about the tradeoffs in practice.[179] For this reason, among others, there is increasing interest among US regulators in shifting the burden from consumers to data holders. This shift can be seen, for instance, in the White House's recent *legislative proposal* for implementing and enforcing a consumer privacy bill of rights, which requires commercial entities to process personal data in a manner that is reasonable in light of the context in which it was collected.[180]

V. Conclusions

Based on the discussion of two leading use cases at the current frontier of digital development, Big Data and the Internet of Things, the first part of this paper called for an *ecosystem perspective* in order to adequately contextualize the digital privacy crisis, which is an expression of larger shifts in today's information-based society. The approximate and tentative analysis of some of the key factors at play paints a picture in which the current status of digital privacy is a result of a complex interplay among various elements, including technological advancement, economic and market drivers, user behavior, and legal forces, with a multitude of corresponding actors and a variety of vectors that point in different directions.

In short, four main features characterize the ecosystem in which the digital privacy crisis has emerged and in which it needs to be addressed. Frist, even a brief and incomplete scan and analysis suggests that the digital privacy phenomenon unfolds in a *complex system* environment. The complexity of the technological systems ranging from Big Data analytics to the Internet of Things has been widely recognized. A prominent and perhaps more familiar example are search algorithms such as Google's PageRank, which may reach a degree of complexity that goes beyond what the creators and owners of the technology can control – a growing issue of concern with respect to the *accountability of*

179 Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, Harvard Law Review, Vol. 126, pp. 1880–1903, 2013. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018>.

180 U.S. White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, 2015, Sec. 104(a). <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>.

algorithms.[181] In addition to the inherent complexity of each cluster of elements such as technology, markets, human behavior, and law, it is the vast web of often invisible links that connect these elements with each other and with the many stakeholders involved – across cultures and jurisdictions – that exacerbates the overall complexity of the digital ecosystem in which digital privacy and its future is situated.[182]

This already indicates a second challenge that is related to the complexity issue: the problem of *limited transparency*. Many of the technological processes involved in the collection and usage of information – including personal data – are invisible to the individuals involved, leading to a systemic problem of incomplete and asymmetric information, which puts limits on certain approaches when considering the future of digital privacy, as further discussed below. The lack of transparency applies not only to the technological factors, but also to other important drivers in the ecosystem. For instance, the incentive structure of the various actors involved is not always clearly visible and might change dynamically over time based on feedback loops and larger shifts in privacy awareness. Along similar lines, many of the causalities remain unclear – for example the indirect downstream effects of non-privacy specific legal interventions at the higher level of technological systems, such as cloud computing,[183] on digital privacy.

A third feature of the digital ecosystem that is relevant with respect to the future of digital privacy is the dynamic nature or *fluidity* of the space. Whether rapid technological advancements, evolving business models, changing user behavior, or laws that are in flux, the ecosystem discussion suggests many moving elements, which not only shape the level of digital privacy protection or threat, but also influence the very notion of privacy itself, which makes it chronically difficult to define what (digital) privacy means.[184] These changing notions of privacy, in turn, are likely to shape the future design of technology and legal frameworks, as recent draft legislation in the US illustrates,[185] which

---

181 See, e.g., Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Cambridge and London 2015.

182 See also Palfrey/Gasser (n. 10), Chapter 8: Complexity.

183 See, e.g., Millard (n. 161).

184 Julie Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, New Haven 2012, Chapter 5: Privacy, Autonomy, and Information; see also, Caroline Golin, Impressions of Privacy in the Media: Does Greater Public Awareness of Privacy Concerns Influence Legislative Action? Georgia Institute of Technology, 2012. <http://papers.ssrn.com/abstract=2204447>. For a concise overview of the different privacy theories and their evolution over time, see, e.g., Judith DeCew, Privacy, Edited by Edward N. Zalta, The Stanford Encyclopedia of Philosophy, 2015. <http://plato.stanford.edu/archives/spr2015/entries/privacy/>; see also Adam D. Moore, Defining Privacy, Journal of Social Philosophy, Vol. 39, No. 3, pp. 411–28, 2008; and Daniel J. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3, pp. 477–560, January 2006. <https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf>.

185 U.S. White House (n. 180).

is reflective of privacy as contextual integrity as one of the latest theoretical models of privacy mapping technological advancements and societal evolution.[186]

Taken together, these and related phenomena create considerable levels of *uncertainty* with respect to the future of the digitally networked environment in general, and digital privacy in particular. From such an ecosystem perspective, uncertainty not only arises for users from incomplete and asymmetric information, but also affects designers and policymakers both in the public and corporate sector, who through their choices shape the evolution and future direction both of the overall ecosystem, as well the parameters of digital privacy more specifically. Against this backdrop, any regulatory intervention – broadly defined – in the digital space has to deal with the typical conditions of uncertainty that are characteristic of the networked world,[187] which increases the importance of designing and implementing *mechanisms of learning* as more information and better knowledge might become available in the future.[188]

C. Approaches to the Future of Digital Privacy

I. Overview

The previous sections suggest that digital privacy can only be appropriately understood as the result and in the context of larger technological, economic, behavioral, and legal shifts over the past decades that constitute and shape today's digitally networked environment. Such a phenomenon-oriented perspective helps make visible and explain the extraordinary complexity and scale of the digital privacy challenges introduced in the first part of the report. It also indicates that an exploration of the *solution space* when addressing the future of digital privacy needs to expand beyond legal approaches in general and (traditional) privacy laws in particular.

A possible conceptual starting place when mapping and clustering the approaches available to shape the future of privacy in the digital age and manage the multi-faceted, multi-layered, and multi-actor digital privacy challenges

---

186 Helen Nissenbaum, Privacy as Contextual Integrity, Washington Law Review, Vol. 79, No. 1, pp. 119–158, February 2004. <http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf>; Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford 2009.

187 With respect to law, see, e.g., Karl-Heinz Ladeur, Postmoderne Rechtstheorie: Selbstreferenz, Selbstorganisation, Prozeduralisierung, Zweite, mit einem Nachwort versehene Auflage, Berlin 1995; and his contributions in Karl-Heinz Ladeur, Das Recht der Netzwerkgesellschaft, hrsg. von Thomas Vesting and Ino Augsberg, Tübingen 2013.

188 See, e.g., Urs Gasser, Legal Frameworks and Technological Protection of Digital Content: Moving Froward towards a Best Practice Model, Berkman Center Research Publication No. 2006–04, June 2006. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=908998>.

characterized by high degrees of uncertainty, fluidity, and complexity, is an influential framework that builds upon the Chicago School and was adapted by Professor Lawrence Lessig to address regulatory problems in the digitally networked environment. The framework, outlined in Lessig's seminal book «Code and Other Laws of Cyberspace,»[189] identifies *four modes of regulation* that constrain human behavior: architecture (which Lessig terms «code» in the context of cyberspace), markets, social norms, and law, which correspond with the key ecosystem factors analyzed in the preceding section of this report.

Over the past decades, the four-modes-of-regulation model has greatly influenced the ways in which privacy and public policymakers approach regulatory problems in the Internet age.[190] In the digitally networked environment, which heavily depends on software, «code» is considered to be a particularly powerful force to shape behavior, making the online world – contrary to mainstream opinion – potentially more «regulable» than the offline world. Code has been recognized as an effective mechanism to achieve certain goals and is applied by legislators and courts in a broad variety of situations, ranging from technological protection of copyrighted digital content to the blocking of illegal online content such as child pornography. These examples indicate another important aspect of the framework: different modes of regulation interact with each other and, more often than not, have to be woven together to form a *blended governance approach* in order to achieve the desirable outcomes – a process in which law plays an important role and achieves desired effects both directly and indirectly.[191]

Despite the interaction among the different modes of regulation and blurring lines among them, in addition to deeper-layered conceptual limitations of the four-forces model,[192] the framework is used in this section as a *navigation aid* to map and discusses – again with an eye towards the future and under the particular ecosystem conditions identified in the previous section – the different approaches to the future of digital privacy. Each approach examined (others could be added) is briefly characterized, illustrated in its application by referring back to the leading use cases – Big Data and Internet of Things – provided in the first part, and discussed in terms of promise and limitations. Each subsection ends with a brief outlook.

---

189 Lessig (n. 13).

190 See, e.g. Weber (n. 14), pp. 53–89.

191 See, e.g., Weber (n. 14), pp. 92–94 with disucssion of similar mixed approaches by Paul Schiff Berman, Global Legal Pluralism, South California Law Review, Vol. 80, pp. 1155–1237, 2007; François Ost and Michel van de Kerchove, De la pyramide aux réseau? Pour une théorie dialectique du droit, Bruxelles: Presses des Facultés Universitaires Saint Louis, 2002; Emily Weitzenboeck, Hybrid Net: The Regulatory Framework of ICANN and the DNS, International Journal of Law and Information Techology, Vol. 22, pp. 49–73, 2014.

192 Viktor Mayer-Schönberger, Demystifying Lessig, Wisconsin Law Review, No. 4, pp. 713–746, 2008. <http://hosted.law.wisc.edu/lawreview/issues/2008_4/mayer-Schönberger_-_final.pdf>.

II. Technology-Based Approaches

1. Approach

a. Privacy-Enhancing Technologies

Starting in the 1970s, researchers began to propose technical mechanisms as means to respond to the privacy and data protection challenges emerging from new information and communication technologies.[193] Among the earliest discussions of technology-based approaches to the emerging challenges was a report published by the data protection agencies of the Netherlands and Ontario, Canada, in which the concept of so-called *Privacy Enhancing Technologies* (PETs) was explored.[194] The report addressed the question of what «conditions must be kept in mind when engineering an information system in order to guarantee that the system can be used effectively and efficiently without revealing the user's identity,» and, specifically, «[w]hat types of information and communication technology can contribute towards achieving this goal.»[195] The study was focused on the conceptualization and use of «identity protectors» to develop privacy-protecting information systems.

Initially, PETs had a rather specific and limited meaning by focusing on a category of technologies aimed at *minimizing* the collection and processing of personal data without losing the functionality of an information system.[196] Policymakers also picked up on this early concept of PETs. The European Commission, for instance, issued a widely referenced Communication in 2007 to promote the use of PETs, in which it referred to the original meaning of PETs as «a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system.»[197] However, the Communication also illustrates how the scope of PETs has broadened over the years, by including not only identity protection, but also encryption tools, cookie cutters, and data management protocols, among others.[198] As the meaning and ap-

---

193 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 1.

194 Office of the Information & Privacy Commissioner of Ontario, Privacy-Enhancing Technologies: The Path to Anonymity (Volume 1), Registratiekamer of the Netherlands, August 1, 1995. <https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329>.

195 Office of the Information & Privacy Commissioner of Ontario (n. 194), p. 1.

196 John J. Borking and Charles D. Raab, Laws, PETs and Other Technologies for Privacy Protection, The Journal of Information, Law and Technology (JILT), No. 1, February 28, 2001. <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/>.

197 Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM (2007) 228 final, May 2, 2007. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0228>.

198 See also Ira Rubinstein, Regulating Privacy by Design, Berkeley Technology Law Journal, Vol. 26, pp. 1409–1456, 2011. <http://ssrn.com/abstract=1837862>.

plication of PETs have broadened, the term has become more amorphous and today lacks a generally accepted definition.

Since the initial concept studies of PETs, a large body of research has explored the development and integration of various technologies as a means to build privacy into information systems.[199] The European Union Agency for Network and Information Security (ENISA) report on Privacy and Data Protection by Design from December 2014 describes a number of PETs that can serve as effective privacy techniques.[200] For instance, Just Fast Keying (JFK) is an example of an authentication protocol with state-of-the-art capabilities as it «provide[s] protections against attacks [... by] third parties from inferring the identities of authenticating parties, do[es] not leak those identities through impersonation, and cannot infer the identity of parties in a secure session,» all of which are risks that jeopardize secure user authentication.[201] Attribute-based credentials are cited as alternatives to traditional identity management techniques: while the latter rely on online identity providers that serve as intermediaries between the individual user and service provider, the former do not, thereby avoiding some of the privacy concerns that arise by having intermediaries that could possibly access individual user's information without his/her consent or knowledge.[202] Other examples include tools for encryption,[203] communication anonymity and pseudonymity,[204] privacy in databases,[205] statistical disclosure control,[206] data user and owner privacy,[207] and storage privacy.[208]

As the range of available PETs has diversified over the years, researchers have developed a series of typologies to group the growing number of PETs. Among others, the categorizations include *taxonomies* based on the life cycle

---

199 See, e.g., European Union Agency for Network and Information Security (ENISA) (n. 57), pp. 22–47.

200 European Union Agency for Network and Information Security (ENISA) (n. 57), pp. 22–47.

201 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 22.

202 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 24.

203 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 27.

204 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 29.

205 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 31.

206 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 32.

207 European Union Agency for Network and Information Security (ENISA) (n. 57), pp. 37–38.

208 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 40.

model of data, the different types of privacy harms,[209] the interactions between subjects relating to objects within information systems,[210] or the functionality of PETs.[211] More recently, Rubinstein provided a classification of PETs in terms of their relationship to government regulations, differentiating between two main types of PETs:[212] substitute PETs, which «seek to protect privacy by blocking or minimizing the collection of personal data, thereby making legal protections superfluous;»[213] and complementary PETs, which «are designed to implement statutory privacy principles or related legal requirements.»[214] The distinction between substitute and complementary PETs has proven to be particularly useful when analyzing the (limited) adoption of PETs by the private sector – despite the endorsement of regulators – and understanding the underlying incentive problems, which are further discussed below.

b. Privacy by Design

As noted above, PETs have played a prominent role in privacy debates over the past two decades and have long been embraced by privacy officials both in Europe and the US. However, as one recent report puts it, some «may have misunderstood PETs as the panacea that could solve all privacy problems simply by adding PET components on top of an existing system.»[215] Some clarification at the conceptual level was arguably achieved through the introduction of an overarching philosophy called *Privacy by Design* (PdD) that puts PETs into a larger design and operational context, and embeds them in a series of foundational principles. Pioneered by Ann Cavoukian in the 90s[216] and adopted by the International Conference of Data Protection and Privacy Commissioners in 2010,[217] Privacy by Design can be understood as a «systematic approach to designing

---

209 Yun Shen and Siani Pearson, Privacy Enhancing Technologies: A Review, HPL-2011-113, August 6, 2011. <http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf>.

210 Herbert Burkert, Privacy-Enhancing Technologies: Typology, Critique, Vision, in: Urs Gasser (Hrsg/ed.), Informationsrecht in «E»-Umgebungen, Information Law in eEnvironments, pp. 71–89, Zurich 2002.

211 Ian Goldberg, Privacy-Enhancing Technologies for the Internet, II: Five Years Later, in: Privacy Enhancing Technologies, pp. 1–12, Berlin 2003. <http://freehaven.net/anonbib/cache/fiveyearslater.ps>.

212 Rubinstein (n. 198), p. 1416.

213 Rubinstein (n. 198), p. 1417. Prominent examples of PETs that are aimed at minimizing data collection and analysis include applications such as anonymous web browsing or encrypted email as adopted by end-users.

214 Rubinstein (n. 198), p. 1418. Complementary PETs can further be grouped in privacy-friendly PETs that seek to give people more control over their data (e.g. through digital dashboards, browser management tools, etc.), and privacy-preserving PETs, which typically rely on elaborate cryptographic methods. Rubinstein (n. 198), pp. 1418–1419.

215 European Union Agency for Network and Information Security (ENISA) (n. 57), p. 5.

216 Ann Cavoukian, Privacy by Design, January 27, 2009. <https://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf>.

217 32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, Jerusalem, Israel, October 27–29, 2010. <https://secure.edps.eu

any technology that embeds privacy into the underlying specifications or architecture.»[218] Although Cavoukian first conceived of the principle to apply to information technologies, she expanded its use to «(2) business practices; and (3) physical design and infrastructures.»[219]

As an overarching approach, Privacy by Design clarifies that PETs are one specific instrument in the toolbox to address certain dimensions of a given privacy problem, such as anonymity in the context of payment or communication systems. At a *fundamental* level, Privacy by Design «prescribes that privacy be built directly into the design and operation, not only of technology, but also how a system is operationalized (e.g., work processes, management structures, physical spaces and networked infrastructure).»[220]

At the *implementation* level, Privacy by Design remains amorphous and has been interpreted differently. Although Cavoukian articulates seven guiding principles for the implementation of Privacy by Design,[221] Ira Rubinstein argues that they provide little instructions in translating Privacy by Design into actual engineering practices; instead, «[a]t the very least, [Privacy by Design] means implementing FIPPs [Fair Information Practice Principles] in the design and operation of products and services that collect, or in any way process, personal data.»[222] FIPPs, which are substantive principles advocated by the FTC such as data security, reasonable collection limits, sound retention practices, and data accuracy,[223] thus constitute additional guidelines to implement Privacy by Design.[224] Nevertheless, these principles are arguably vague and lack

---

ropa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf>.

218 Rubinstein (n. 198), pp. 1411–1412.

219 Cavoukian (n. 216). See also Cavoukian's application of Privacy by Design to specific technologies, such as smart meters; Ann Cavoukian and Klaus Kursawe, Implementing Privacy by Design: The Smart Meter Case, 2012 International Conference on Smart Grid, August 2012; home health care technologies, Ann Cavoukian, Michelle Chibba and Alex Stoianov, Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment, The Review of Policy Research, Vol. 29, No. 1, pp. 37–61, January 2012; and business practices in general, Ann Cavoukian, Scott Taylor and Martin Abrams, Privacy by Design: Essential for Organizational Accountability and Strong Business Practices, Identity in the Information Society, Vol. 3, No. 2, pp. 405–413, 2010.

220 Ann Cavoukian and Jeff Jonas, Privacy by Design in the Age of Big Data, June 8, 2012, p. 9. <https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf>.

221 The seven principles are: «1. Recognition that privacy interests and concerns must be addressed proactively; 2. Application of core principles expressing universal spheres of privacy protection; 3. Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle –end to end; 4. Need for qualified privacy leadership and/or professional input; 5. Adoption and integration of privacy-enhancing technologies (PETs); 6. Embedding privacy in a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality; and 7. Respect for users' privacy.» Cavoukian (n. 216), p. 1.

222 Rubinstein (n. 198), p. 1421.

223 U.S. Federal Trade Commission (FTC) (n. 56), p. 23.

224 U.S. Federal Trade Commission (FTC) (n. 56), p. 30. Procedural protections complement and implement these substantive principles: the FTC states that «[c]ompanies should maintain

guidance for companies and engineers to translate Privacy by Design into tangible tools or measures to effectuate privacy protection. Alternatively, others interpret the concept as a life cycle approach to software development and data management, or envision its implementation in the context of risk-based privacy assessments and privacy management programs.[225]

Despite (or maybe because of) the lack of conceptual clarity, *policymakers and regulators* on both sides of the Atlantic have embraced Privacy by Design as a concept based on the premise «that existing regulation and policy alone are not fully sufficient to safeguard privacy.»[226] In the US, the Final FTC Privacy Framework establishes Privacy by Design as a best practice by calling companies to «promote consumer privacy throughout their organizations and at every stage of the development of their products and services,»[227] adopting a broad meaning of the concept. To shift burdens away from consumers and place obligations on businesses to treat consumer data in a privacy-responsible manner, the report outlines both substantive and procedural principles: it calls upon companies to incorporate privacy protections into their practices and maintain comprehensive data management procedures throughout the life cycle of their products and services. Importantly, the FTC has also mandated Privacy by Design in several recent consent decrees, as further discussed below.

Privacy by Design is also highlighted in the 2009 Article 29 Working Party report on «The Future of Privacy,»[228] and in the Commission Communication on «A Digital Agenda for Europe,» where it is defined as a principle that «means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.»[229] The proposed EU General Data Protection Regulation also embraces the design approach. While the exact wording is still in flux,[230]

---

comprehensive data management procedures throughout the life cycle of their products and services.»

225 See for an overiw Ira Rubinstein and Nathan Good, Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, 28 Berkeley Technology Law Journal, pp. 1333–1414, 2013, p. 1139. <http://ssrn.com/abstract=2128146>. Under this view, Privacy by Design refers more broadly to the «adoption of processes, systems, procedures, and policies —any of which may also have a technological dimension—and which may be referred to collectively as privacy safeguards» as the EU has done by adopting «sound design practices» in addition to the use of PETs; Rubinstein (n. 198), p. 1421.

226 32nd International Conference of Data Protection and Privacy Commissioners (n. 217), p. 1.

227 U.S. Federal Trade Commission (FTC) (n. 57), p. vii.

228 Article 29 Data Protection Working Party/Working Party on Police and Justice (n. 62), pp. 12–15.

229 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. <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01)>.

230 See European Parliament Legislative Resolution of 12 March 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Re-

Article 23 sets forth the principles of data protection by design and default, and requests, in essence, that data controllers implement both technical and organizational measures to meet the requirements of the regulation and protect the rights of the data subjects. According to the current version, the Commission might lay down the appropriate technical standards, which will ultimately clarify the meaning of Privacy by Design in practice.

In Switzerland, the Federal Council has identified Privacy by Design as a key mechanism to achieve one of the goals of the revision of the Swiss Data Protection Act: identify and evaluate data protection problems already at the stage of technology development, to the extent possible and appropriate.[231] In its current version, the Data Protection Act mandates the protection of personal data against unauthorized processing by appropriate technical and organizational measures.[232] The norm on data security, however, primarily aims to prevent unauthorized access to personal data and thus only covers one aspect of Privacy by Design.[233] In this sense, the norm's use of the word «appropriate» means that it does not mandate the absolute or highest possible degree of protection.[234] For instance, encryption of sensitive data – while certainly beneficial to data security – will not generally be required if an acceptable level of security is achieved by other means; rather the appropriate measures will be assessed depending on the relevant context and on a case-by-case basis.[235]

As instructed by the Data Protection Act,[236] the Federal Council has included minimal requirements for data security in the Ordinance on Data Protection, besides listing a series of risks to be addressed by the measures such as accidental deletion, loss of data, or unauthorized processing.[237] The Ordinance also frames a set of broad criteria to which the technical and organizational measures need to adhere.[238] These criteria, however, do not represent Privacy by Design as described above.

Whereas the overhaul of the Data Protection Act is still pending, politicians have called for the concept of Privacy by Design to be introduced to Swiss data

---

gard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2014. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014–0212+0+DOC+XML+V0//EN>

231 Schweizerischer Bundesrat, Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz, December 9, 2011, p. 350. <http://www.admin.ch/opc/de/federal-gazette/2012/335.pdf>.

232 Art. 7 para 1 Swiss Data Protection Act.

233 See Kurt Pauli, Art. 7 – Datensicherheit, in: Urs Maurer-Lambrou and Nedim Peter Vogt, Basler Kommentar Datenschutzgesetz, pp. 114–125, Basel 2006.

234 See David Rosenthal and Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Art. 7 Datensicherheit, Zürich 2008, Art. 7 N 3.

235 Rosenthal/Jöhri (n. 234), Art. 7 N 4.

236 Art. 7 para. 2 Swiss Data Protection Act.

237 Art. 8 para. 1 Data Protection Ordinance.

238 Art. 8 para. 2 Data Protection Ordinance.

protection law.[239] Similarly, the advisory group for the revision of the Act has suggested introducing Privacy by Design as due diligence for data processors.[240] While some experts do not necessarily view the codification of Privacy by Design as the ideal solution and favor the promotion of self-regulation in the respective industries,[241] the Federal Data Protection and Information Commissioner proposed evaluating whether Privacy by Design should be enshrined in law in order to ensure that redundant acts of data processing would a priori be rendered impossible, and for consumers to be granted the security of receiving products and services that are oriented towards privacy by default.[242] Preempting said review of the Act, the Federal Data Protection and Information Commissioner has developed a tool to analyze the impact of new products and services regarding data protection already in the planning stage.[243] The dynamic survey is aimed at raising awareness for Privacy by Design outside of legal requirements.

2. *Application*

a. *Big Data*

From a *conceptual* angle, privacy and data protection authorities have promoted the Privacy by Design approach to address some of the thorny Big Data privacy challenges outlined in the introduction section. The pioneer of a pro-active design approach to privacy, Ann Cavoukian, is again among the leading advocates propagating the idea that technologists should embrace Privacy by Design as a way to deliver responsible innovation in the age of Big Data.[244] Similarly, scho-

---

239 See, e.g., Jean Christophe Schwaab, Drei Vorschläge, wie der Datenschutz verbessert werden kann, Gastkommentar zum Datenschutz, Neue Zürcher Zeitung, July 30, 2014. <http://www.nzz.ch/meinung/debatte/drei-vorschlaege-wie-der-datenschutz-verbessert-werden-kann-1.18353986>.

240 See Federal Office of Justice, Normkonzept zur Revision des Datenschutzgesetzes: Bericht der Begleitgruppe Revision DSG, October 29, 2014, pp. 18–22. <http://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf>.

241 See, e.g., Rehana Harasgama and Aurelia Tamò, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: Rolf H. Weber and Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, ZIK Nr. 59, pp. 117–149, Zürich 2014, p. 147. See also Robert Baumann, Mehr Datenschutz in Europa, digma – Zeitschrift für Datenrecht und Informationssicherheit, pp. 116–121, 2013, p. 117.

242 See Thür, (n. 81), p. 97.

243 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 21. Jahresbericht, 2013/2014, p. 65 et seq. <http://www.edoeb.admin.ch/dokumentation/00153/01174/index.html>. The Commissioner had previously also pointed out that Privacy by Design urgently needs to be considered during the development of new services and products in a report on the collection of payload data in the context of Google Street View trips, see Eidgenössischer Datenschutzbeauftragter, Bericht zur Erfassung von Payloaddaten im Rahmen der Google Street View Fahrten, January 2011. <http://www.edoeb.admin.ch/datenschutz/00683/00690/00694/00695/index.html?lang=de>.

244 See, e.g., Cavoukian/Jonas (n. 220); and Ann Cavoukian, David Stewart and Beth Dewitt, Using Privacy by Design to Achieve Big Data Innovation Without Compromising Privacy,

lars have proposed Privacy by Design in the Big Data context, both as a horizontal way to deal with privacy risks as well as with respect to specific Big Data applications such as search engines and smart meters, among others.[245] Regulators have also called for a pro-active and design-based approach to Big Data privacy risks, both in policy reports and draft legislation. More concretely and as briefly mentioned above, the FTC has mandated Privacy by Design in several consent decrees, most notably in a settlement with Google.[246] As a leader in the Big Data business, the company is required to implement a comprehensive privacy program that addresses privacy risks related to the development and management of consumer products and services by conducting comprehensive privacy risk assessments and implementing reasonable privacy controls and procedures.

From an *implementation* perspective, however, a significant gap remains between the relatively abstract request for Privacy by Design in Big Data environments and practical application.[247] However, a rapidly expanding series of case studies covering a diverse set of Big Data scenarios such as sense-making systems, electronic petition systems, electronic toll pricing, and mobile data publishing provides insight and guidance into how Privacy by Design can be applied in practice. A growing body of literature seeks to synthesize lessons learned across these implementations and generalizes these findings to the extent possible.[248] In addition to such bottom-up efforts, privacy experts have started to operationalize internationally recognized privacy principles and use

---

pp. 1–26, June 10, 2014. <https://www.ipc.on.ca/images/Resources/pbd-big-data-innovation_Deloitte.pdf>.

245 See, e.g., Patrick Eggimann and Aurelia Tamò, Taming the Beast: Big Data and the Role of Law, in: Big Data and Privacy: Making Ends Meet, Conference Proceedings, pp. 27–30, 2013. <http://www.futureofprivacy.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf>; Ryan Calo, Consumer Subject Review Boards: A Thought Experiment, Stanford Law Revview Online, Vol. 66, pp. 97–102, 2013. <http://www.stanfordlawreview.org/sites/default/files/online/topics/Calo.pdf>.

246 U.S. Federal Trade Commission (FTC), In the Matter of Google Inc. (File No. 102 3136, 2011). <http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf>.

247 See, e.g., Anna Monreale, Salvatore Rinzivillo, Francesca Pratesi, Fosca Giannotti and Dino Pedreschi, Privacy-by-design in Big Data Analytics and Social Mining, EPJ Data Science, 2014. <http://www.epjdatascience.com/content/3/1/10>; and more generally Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn and Ron van Paassen, Designing Privacy-by-Design, in: Bart Preneel and Demosthenes Ikonomou (eds.), Privacy Technologies and Policy, pp. 55–72, Lecture Notes in Computer Science, 8319, Berlin 2014. <http://link.springer.com/chapter/10.1007/978-3-642-54069-1_4>; Seda Gürses, Carmela Troncoso and Claudia Diaz, Engineering Privacy by Design, Computers, Privacy & Data Protection, 14, 2011. <https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf>. For a Swiss perspective, see also Bruno Baeriswyl, Privacy Enhancing Technologies (PET) versprechen (zu) viel bei der Umsetzung von neuen Technologien, digma – Zeitschrift für Datenrecht und Informationssicherheit, pp. 18–21, 2012.

248 See, e.g., Schwaab (n. 239).

them in the (counterfactual) analysis of recent privacy incidents involving large data sets.[249]

In addition, researchers and practitioners focus on the development and application of specific tools and techniques to address particular dimensions of the Big Data privacy challenge, including mechanisms that provide access control to data, manage identities, enable privacy-preserving analysis, or facilitate interactions and transactions.[250] Some of these techniques – such as state-of-the-art authentication protocols – are well developed, have their historic roots in the PETs discussed above, and may build on international *standards* such as ISO.[251] Others, such as advanced statistical and computational techniques, that seek to address new privacy challenges that specifically arise in the context of analyzing very large datasets are currently under development.[252] Examples of emerging computational approaches include secure multi-party computation,[253] a technique for the joint analysis of data from multiple sources while ensuring the input data remain private; functional or homomorphic encryption,[254] which makes it possible to analyze data stored in encrypted files; and differential privacy,[255] a formal mathematical framework for privacy-preserving data analysis. Theoretical advances in these areas, if successfully brought to practice, may enable Big Data processing and analytics that do not reveal privacy-sensitive information about individuals.[256]

In Switzerland, the Data Protection Ordinance provides a set of goals to be pursued by the owners of large data collections through the implementation of technical and organizational measures.[257] These goals include controlling access to and transport of data, among other things. Swiss Federal law currently also provides that data collections are to be registered with the Federal Data Protection and Information Commissioner if 1) they contain sensitive personal

---

249 Rubinstein/Good (n. 225).

250 For an overview, see, e.g., Carl Landwehr, Engineered Controls for Dealing with Big Data, in: Julia Lane, Vicotria Stodden, Stefan Bender, Helen Nissenbaum (eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, pp. 211–233, Cambridge 2014.

251 See, e.g., European Union Agency for Network and Information Security (ENISA) (n. 61), p. 22 et seq.

252 See, e.g., Cynthia Dwork, Differential Privacy: A Cryptographic Approach to Private Data Analysis, in: Julia Lane, Vicotria Stodden, Stefan Bender, Helen Nissenbaum (eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, pp. 296–322, Cambridge 2014.

253 See, e.g., Yehuda Lindell and Benny Pinkas, Secure Multiparty Computation for Privacy-Preserving Data Mining, Journal of Privacy and Confidentiality, Vol. 1, No. 1, 2009.

254 See generally Brian Hayes, Alice and Bob in Cipherspace: A New Form of Encryption Allows You to Compute with Data you Cannot Read, American Scientist, 2012. <http://www.americanscientist.org/issues/pub/alice-and-bob-in-cipherspace>.

255 See, e.g., Dwork (n. 252).

256 See generally Sophia Yakoubov, Vijay Gadepally, Nabil Schear, Emily Shen and Arkady Yerukhimovich, A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud, IEEE High Performance Extreme Computing Conference, 2014. <http://www.ieee-hpec.org/2014/CD/index_htm_files/FinalPapers/28.pdf>.

257 Art. 9 Para. 1 Data Protection Ordinance.

data or personal profiles or 2) personal data is regularly shared with third parties.[258] Owners of such data collections are exempt from registration if they have attained a certificate for quality of data protection, for instance the standard for information security systems, ISO/IEC 27001:2013.[259] The Federal Data Protection and Information Commissioner has issued minimal requirements that must be met in order for such data protection management systems to be recognized for valid certification (based on the Ordinance on Data Protection Certification).[260] The guidelines for minimal requirements closely follow ISO/IEC 27001:2013; their Annex even goes as far as to refer to Annex A to ISO/IEC 27001:2013, which incorporates the maxim amount Privacy by Design measures to be implemented for the sake of data security within project management.[261]

While such implementation of state of the art standards for data protection through law takes an approach similar to Privacy by Design – as it requires that data protection be implemented in data management systems – Switzerland is yet to enshrine the concept in law.

b. Internet of Things

One component of the Internet of Things is *Radio-Frequency Identification* (RFID) tags, which enable the automatic and remote identification of objects. As noted in the introduction, these technical characteristics of RFIDs, and the widespread use, triggered strong privacy concerns and even led to consumer boycotts.[262] In response, privacy and security researchers developed a broad range of PETs with an initial focus on control over the RIFD read process and the goal of preventing unauthorized access to RFID tags.[263] An early review of hundreds of papers on PETs for RFID demonstrates the various ways in which the privacy and security community developed technology-based approaches to the particular privacy challenge of RFIDs as the enabling component of the Internet of Things. Techniques include a «kill switch» to simply disable an RFID

---

258 Art. 11a Para. 3 a) and b) Data Protection Act. Note, however, that the advisory group for the revision of the Data Protection Act suggests to drop the mandatory register, see FEDERAL OFFICE OF JUSTICE (n. 240), p. 29.

259 Art. 11 Para. 1 and Art 11a Para. 5 f) Data Protection Act. The accreditation of organizations giving out such certificates is governed by the Ordinance on Data Protection Certification. For the details of information security standard ISO/IEC 27001:2013; see also <http://www.iso.org/iso/catalogue_detail?csnumber=54534>.

260 See the guidelines on the minimum requirements for data protection management systems (in German) at <http://www.edoeb.admin.ch/datenschutz/00756/index.html?lang=de>.

261 See para. G.1 of the Annex to the guidelines on the minimum requirements for data protection management systems (version of April 15, 2014).

262 See, e.g., SARAH SPIEKERMANN and SERGEI EVDOKIMOV, Privacy Enhancing Technologies for RFID – A Critical State-of-the-Art Report, 2009. <http://www.avoine.net/rfid/download/papers/SpiekermannE-2009-ieeeprivsec.pdf>.

263 SPIEKERMANN/EVDOKIMOV (n. 262), p. 4.

tag's ability to transmit information as they leave the point of sale to more nuanced schemes such as the use of privacy agents or on-tab schemes.[264]

Technological measures, as a way to deal with privacy and data protection concerns, have emerged beyond the initial focus on RFID tags and reads. Swiss experts, for instance, have identified and critically examined a broader range of technological possibilities to increase security and privacy in the Internet of Things environment – including Virtual Private Networks, Transport Layer Security, DNS Security Extensions, Onion Routing, Private Information Retrieval, and Peer-to-Peer systems, among others.[265] As one example, techniques are being developed in the context of smart meter management that would provide utility companies with billing amounts but not detailed energy consumption profiles for individuals.[266]

More broadly, policymakers and regulators both in the US and the EU have promulgated measures that resemble a Privacy by Design approach in the context of the Internet of Things. For instance, the European Data Protection Supervisor identified the need for Privacy by Design for RFIDs in 2008 in an official opinion.[267] Subsequently, the European Commission asked Member States to ensure that the industry – in collaboration with other stakeholders – develops a framework for privacy and data protection impact assessment.[268] The framework, which provides guidance to RFID operators by helping them identify, assess, and address privacy risks, was adopted by a number of industry associations in 2011 and subsequently endorsed by the Article 29 Working Party.[269] Certain technical standards aimed at guiding RFID application operators how to run privacy impact assessments (PIA) in specific fields became a European Norm in 2014.[270] Recently, DG Connect released an internal report

---

264 Spiekermann/Evdokimov (n. 262), pp. 4–5.

265 Rolf H. Weber and Romana Weber, Internet of Things: Legal Perspectives, Zurich 2010, pp. 47–51.

266 See, e.g., Marek Jawurek, Martin Johns and Florian Kerschbaum, Plug-in Privacy for Smart Metering Billing, Proceedings of the 11th International Symposium on Privacy Enhancing Technologies, 2011. <http://freehaven.net/anonbib/papers/pets2011/p11-jawurek.pdf>.

267 Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ‹Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96, OJ C101, Section 42 (23 April 2008). <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008XX0423(01)&from=EN>.

268 See point 4 of Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification, C, 2009. <file:///Users/urstemp/Downloads/CommissionRecommendation2009387EC.pdf>.

269 See Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Adopted February 11, 2011. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf>.

270 Rolf H. Weber, Privacy Impact Assessment – A Privacy Protection Improvement Model? 25th IVR World Congress, Law Science and Technology, Paper Series No. 039/2012, Series B, August 2011, p. 11. <http://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/docId/24897>

on the implementation of the original recommendations, concluding that, «the implementation of the RFID Recommendation as a whole and of the PIA framework in particular remains very limited.»[271] Given a corresponding recommendation by the advisory group for the revision of the Data Protection Act, Swiss privacy law is likely to make a PIA mandatory for data processors if there is a substantial risk for violations of privacy.[272]

Privacy by Design has also been promoted by US regulators as one of the key responses to the privacy challenges associated with the Internet of Things. A recent FTC Staff Report on this topic and with focus on privacy and security in a connected world, for instance, highlighted the importance of design approaches both in the context of security and privacy.[273]

3. Evaluation

a. Promise

The discussion of the use and implementation of the Privacy by Design approach to Big Data and the Internet of Things suggests a great promise of technology-based approaches in response to the multi-faceted privacy and data protection challenges that accompany these phenomena. Some of the key advantages (as well as limitations, see below) of such a design approach aimed at *building-in privacy* have already become visible in the context of PETs. Broadly speaking, PET design creates «a burden of legitimatization on those who want to have personal information in their information systems.»[274] It takes pressure off the individual user and shifts it to the system level, as it forces designers to proactively analyze what personal data is actually necessary in a system instead of getting the subject's broad consent for everything they want to do with the data – and hereby overburdening the data subject and undermining the consent principle.[275] Design approaches also have the potential to translate policy issues into engineering language and hence increase semantic interoperability among the different actors involved.

---

describes such a PIAS as a combination of self-regulation and a «code-related» notion («since technology plays a major role»), in which «compliance with the applicable legal framework is supervised by the authorities.»

271 Report on the Implementation of the Commission Recommendation on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification. European Commission, August 27, 2010. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6720>.

272 See Federal Office of Justice (n. 240), p. 20.

273 U.S. Federal Trade Commission (FTC) (n. 56), p. 26 and p. 34.

274 See, e.g., Burkert (n. 210), p. 75.

275 Burkert (n. 210), p. 75. As Weber demonstrates, it would unnecessarily complicate contract negotiation if we would step away from giving consent on the basis of general terms and conditions and have individual contracts for everyone, see Weber (n. 58), pp. 25–26.

Many of these advantages and achievements of PET design, *mutatis mutandis*, also apply to the broader idea of Privacy by Design, which provides *additional* benefits by offering a more holistic approach than PETs and that combine various technological and organizational measures. As noted above, different views exist on how Privacy by Design should be operationalized and applied in practice, and its value proposition is likely to change in detail with each scenario. When interpreting Privacy by Design as a way to translate FIIPs into engineering and usability, for instance, it provides extensive privacy protections at the system level that go far beyond PET's original focus on data minimization. If interpreted as a life cycle approach to software development or data management, reports and scholarly articles demonstrate how technology companies' detailed and rather comprehensive privacy guidelines can indeed play a key role in enhancing privacy for their customers and incorporating the principle into their business models.[276]

In addition to these first order benefits, Privacy by Design also offers second order benefits at the normative level and in terms of *accountability.* It not only strengthens the basis to hold companies responsible for their privacy practices, but also creates additional structural couplings – or interfaces – between the technical and social spheres, as questions about the desirable level of privacy protection can now be discussed more specifically. This feature is particularly important given the potential shift in the very idea of what «privacy» means in today's environment, as noted earlier. Viewed from this angle, Privacy by Design creates an accountability mechanism not only for engineers and companies, but also for policymakers and society at large, which can now shape privacy and data protection policies, procedures, and architectures more directly and granularly by specifying technical standards and/or requiring certain organizational practices, etc.[277]

b. Limitations

The limitations of PETs and design approaches to privacy more broadly have been examined extensively in the literature. Differentiating between internal and external limitations, privacy scholar Professor Herbert Burkert provides a detailed account of the different types of limitations, some of which are inherent in PET designs in general, and others that apply to certain PET concepts but not to others.[278] Among the list of *internal limitations*, one might highlight

---

276 See, e.g., Center for Democracy and Technology, The Role of Privacy by Design in Protecting Consumer Privacy, January 28, 2010. <https://cdt.org/insight/the-role-of-privacy-by-design-in-protecting-consumer-privacy-1/>; Rubinstein (n. 198), pp. 1423–1426; Peter Schaar, Datenschutz in Zeiten von Big Data, HMD Praxis der Wirtschaftsinformatik, Vol. 51, No. 6, pp. 840–852, 2014, p. 849, further notes that implementing Privacy by Design is less expensive than closing privacy loopholes at a later point.

277 This point is inspired by Burkert (n. 210), pp. 76–77, discussing increased political responsibility as an effect of PETs.

278 See, e.g., Burkert (n. 210), pp. 77–84.

three challenges in particular that suggest broader conceptual issues. First, the problem of asymmetric protection: At least some types of PETs build upon the perception that only one party's personal information within an interaction needs to be shielded, not the other, leading to one-directional protection. Second, some PETs rely on the capability to differentiate between identifiable from non-identifiable data; this ability might be challenged in the case of indirectly identifiable information or the unforeseen possibility of establishing identity through combination with other data points. Third, the focus on PET design for one particular system might create a risk of overlooking the interconnectedness of this system with others. On the side of *external factors*, Burkert discusses the limits of PETs to reflect and embrace more fluid and contextual notions of privacy, the tension between PET-enabled anonymity and the social need for mobilization, and the economics of information, according to which personal information is used as a «currency» in return for a service or product.[279]

Economic arguments also play a key role when analyzing the limitations of the Privacy by Design approach. Taking the relatively weak consumer demand for PETs as a factual starting point, Rubinstein identifies a number of reasons for the low adoption rate of these technologies. Reasons include the lack of consumer awareness about privacy risk exposure due to persistent information asymmetries; the existence of a «privacy paradox» and variable privacy sensitivities; and bounded rationality and behavioral biases such as immediate gratification or optimism bias.[280] With respect to the supply side, the economic literature identifies various reasons why firms – absent any government intervention – are arguably reluctant to invest in complementary PETs in particular and Privacy by Design more generally. Rubinstein concludes that in addition to the weak consumer demand for PETs, the «opportunity costs to businesses associated with many PETs, and a lack of relevant data needed for cost-benefit analyses of investments in privacy safeguards all work against the further implementation of PETs in the marketplace.»[281]

Beyond economic arguments, a number of *conceptual challenges* are currently limiting the potential of Privacy by Design specifically. In addition to the fundamental points identified by Burkert, it is the lack of a coherent interpretation of the concept that makes not only its application difficult in practice and at the level of a product or service,[282] but also limits the effectiveness of the approach at the aggregated societal level where different components and sys-

279 See Burkert (n. 210), pp. 77–84.

280 Rubinstein (n. 198), pp. 1433–1435.

281 Rubinstein (n. 198), p. 1444.

282 See, e.g., Gürses/Troncoso/Diaz (n. 247), p. 3 («Despite its comprehensiveness, it is not clear from Cavoukians document, what «privacy by design» actually is and how it should be translated into the engineering practice»); van Rest/Boonstra/Everts/van Rijn/van Paassen (n. 247), p. 56 («The omission of a clear definition of PbD entails that for European citizens,

tems need to interoperate. That said, and as noted before, researchers and policy-makers are working towards more specific frameworks that flesh out what Privacy by Design might mean – a trend that might push the limits of the approach. The guidelines, policies, tools, and systems of large technology companies are another important source to develop good practice when building privacy into software development and data management,[283] which might also interact productively with normative requirements set by regulators.

4. *Outlook*

Going forward, there is little doubt that technology-based approaches aimed at addressing the digital privacy challenges of our time will play an *increasing* role both in private practice and public policy-making. As an approach that emphasizes the need to consider privacy before – not after – the development and use of technology, Privacy by Design offers a more effective approach to addressing privacy concerns than through ex post and ad hoc measures.[284] As discussed, Privacy by Design also has the advantage of operating at the systems level, does not exclusively rely on individuals with bounded rationality, and scales – a series of important features given the nature and scale of the privacy and data protection risks outlined in the earlier parts of this report.

However, the discussion also suggests that the overall performance of Privacy by Design – and technology-based approaches more specifically – will in no small part depend on its *interaction* with appropriate legal and regulatory frameworks aimed at correcting market failures. This immediately creates a complex design challenge for lawmakers that is at least threefold: in order to be effective, legislators and regulators (either through rule-making or enforcement actions) have to provide more specific guidance regarding what Privacy by Design means and requires, while avoiding pitfalls such as creating technological lock-in and path dependencies. Embracing and substantiating Privacy by Design as an approach in innovative legal and regulatory frameworks – for instance using strategies of co-regulation[285]– in turn, will force law- and policy-makers to revisit the dominant theory of privacy as individual control over personal data and embrace concepts that are contextual and contingent.[286] Finally, and perhaps most importantly, it reveals normative dilemmas and value trade-

---

policy makers, authorities and industry it is currently unclear what a request for PbD practically means.»). See also RUBINSTEIN (n. 198), pp. 1414–1415.

283 RUBINSTEIN (n. 198), pp. 1423–1426.

284 See, e.g., RUBINSTEIN/GOOD (n. 225) for a presentation of counterfactual scenarios with Google and Facebook privacy incidents that could have been effectively avoided had the companies accounted for user privacy concerns before developing the problematic products and services.

285 See, e.g., RUBINSTEIN (n. 198), p. 1445.

286 DEIRDRE K. MULLIGAN and JENNIFER KING, Bridging the Gap between Privacy and Design, University of Pennsylvania Journal of Constitutional Law, Vol. 14, No. 4, pp. 989–1034, 2012. <http://ssrn.com/abstract=2070401>.

offs where privacy could be achieved technically, but does not seem acceptable politically.[287]

III. Market-Based Approaches

1. Approach

a. Reputation

A second approach to address privacy and data protection concerns in the age of Big Data and the Internet of Things is to rely on *market-based* mechanisms. In essence, the idea behind this approach is «that reputation and sales of companies will suffer if they offend customers' desires about protecting privacy.»[288] According to the market model, consumer preferences and reputational effects are the main constraints on companies' privacy policies and practices. Consequently, companies will offer products and services that protect privacy to the extent that consumers demand such protections.[289] The more consumers are willing to change purchasing decisions based on privacy policies and practices, the stronger are the disciplining effects of user preferences on companies' privacy behavior.[290]

Reputation shapes a firm's privacy practices because bad publicity – for example in case of a data breach incident – will affect consumer choices and preferences, and drive consumers to alternative and competing offerings.[291] Companies whose core business model is based on the collection and use of sensitive personal data – key actors on the marketplace for personal information – are at the greatest risks of negative reputational effects from a perceived

---

287 For instance, Apple's announcement that it would encrypt iPhones has sparked another controversy over the potential for encryption tools to protect privacy but also hamper law enforcement efforts. See, e.g., Craig Timber, Apple Will No Longer Unlock Most iPhones, iPads for Police, even with Search Warrants, Washington Post, September 18, 2014. The government deplored Apple's new policy as exacerbating the «going dark» problem, in which law enforcement officials lose the ability to lawfully intercept and access communications and information for law enforcement purposes. In contrast, some qualified the government's call to have «backdoors» to obtain data as undermining data security, as such backdoors could not only be exploited by government officials, but also hackers and other unwanted actors. See, e.g., Cory Doctorow, Crypto wars redux: why the FBI's desire to unlock your private life must be resisted, The Guardian, October 9, 2014. <http://www.theguardian.com/technology/2014/oct/09/crypto-wars-redux-why-the-fbis-desire-to-unlock-your-private-life-must-be-resisted>.

288 Peter Swire, Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in: Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce, August 15, 1997. <http://papers.ssrn.com/abstract=11472>.

289 See, e.g. Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age, New York and London 2004.

290 See the discussion in James P. Nehf, Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy, University of Illinois Journal of Law, Technology and Policy, pp. 1–49, 2005. <http://papers.ssrn.com/abstract=1002398>.

291 See generally Swire (n. 288), p. 2.

privacy violation.[292] How powerful such reputational effects are, however, depends largely on the availability of viable alternatives from a user perspective.[293] Overall, the frequency and severity of public privacy violations in recent years have arguably increased the power of reputational effects through heightened user awareness and sensibility.[294]

Negative reputational effects engender significant consequences for companies. Consumer flight and reduction in sales are frequently mentioned in the literature.[295] A practical example that illustrates this effect is the negative business impact of the Snowden revelation on technology companies.[296] Another possible consequence of a negative privacy reputation (typically in combination with other factors) is the failure of certain business models – Google Buzz and Facebook's Beacon service might be illustrative in this respect.[297] Further, negative reputational effects triggered by privacy violations might lead to the dismissal of upper management, as recent news reports about the consequences of large-scale data breaches illustrate.[298]

To avoid these consequences, the theory is that firms should enhance their privacy offerings to prevent any further negative reputational harm. Investments

---

292 See David Matthias Bachmann, A Firm's Reputation as a Regulatory Tool, Diss. University of St. Gallen 2011. <http://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/3904/$FILE/dis3904.pdf>; Swire (n. 288), p. 7 (writing in 1997 that while privacy self-regulation «might promote the reputation of the industry as a whole, and it might facilitate the creation of technical standards that will benefit the industry itself and society more generally,» the opposite might be true.). See e.g. Matt Weinberger, Uber Scandal Highlights Silicon Valley's Bad Behavior, Computerworld, November 18, 2014. <http://www.computerworld.com/article/2849291/uber-scandal-highlights-silicon-valleys-bad-behavior.html>; Johana Bhuiyan and Charlie Warzel, Uber ‹God View': Company Investigates Its Top New York Executive For Privacy Violations, Buzzfeed, November 18, 2014. <http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy –.hgYlZJD44>.

293 See Swire (n. 288), p. 2 (noting that «the more that some or all consumers are willing to change their purchasing decisions based on privacy policies, the greater the market discipline on companies.»)

294 See Grant Gross, Privacy Self-Regulation Efforts are Working, Senators Told, Computerworld, June 28, 2012. <http://www.computerworld.com/article/2505154/e-commerce/privacy-self-regulation-efforts-are-working–senators-told.html>. On the rise and future of the reputation economy more generally, see Michael Fertik, The Reputation Economy, New York 2015.

295 See, e.g., Swire (n. 288), p. 2.

296 See, e.g., Claire Cain Miller, Revelations of N.S.A. Spying Cost U.S. Tech Companies, The New York Times, March 21, 2014. <http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>.

297 See Jaikumar Vijayan, Privacy Advocates Hail Facebooks Plan to Shutter Beacon, Computerworld, September 22, 2009. <http://www.computerworld.com/article/2527870/data-privacy/privacy-advocates-hail-facebook-s-plan-to-shutter-beacon.html>; Greg Sterling, Google: ‹With Buzz We Failed to Appreciate that Users Have Differing Privacy Expectations, Search Engine Land, February 19, 2010. <http://searchengineland.com/google-with-buzz-we-failed-to-appreciate-that-users-have-different-privacy-expectations-36522>.

298 See Bhuiyan/Warzel (n. 292); see also Elizabeth A. Harris, Faltering Target Parts Ways With Chief Following Breach, New York Times, May 5, 2014. <http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html?_r=0>.

in data security aimed at securing personal data of costumers and preventing data breaches, for instance, might be motivated by fear of reputational sanctions such as diminished trust and potential loss of customers – particularly where data breach notification laws require that individuals are informed about data security incidents involving personal information.[299]

In some instances, reputational forces might also lead to gradual adjustments of business strategy and, eventually, the business model. In the rapidly growing space of educational technologies, for instance, anecdotal evidence suggests that at least some technology companies have responded to concerns expressed in the «court of public opinion» by adjusting their information collection practices regarding educational setting and student data.[300] This leads to the next aspect of market-based approaches: the emergence of business model competition on privacy grounds.

b. Business Model Competition

The market model, as described above, suggests that companies will increasingly offer products and services that protect privacy as consumers ask for more of such protections. A version of this argument suggests that consumer demand for privacy drives competition among firms based on their privacy policies and practices, and rewards those firms that will proactively *align their business models* with changing privacy norms.[301] Such businesses will proliferate at pace with consumer demand and capitalize on what has been referred to as the «privacy dividend»[302] or the «privacy payoff.»[303] As a result, the market for privacy might be vitalized based on the emergence of alternative business models. Businesses that do not require the tracking and profiling of consumers may be in the best position to develop business models that are privacy-protective.[304]

---

299 See Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Books and on the Ground, Stanford Law Review, Vol. 63, pp. 247–315, 2011. <http://papers.ssrn.com/abstract=1568385>. See also Sasha Romanosky and Alessandro Acquisti, Privacy Costs and Personal Data Protection: Economic and Legal Perspectives, Berkeley Technology Law Journal, Vol. 24, No. 3, pp. 1060–1100, 2009. <http://papers.ssrn.com/abstract=1522605>.

300 See, e.g., Alistair Barr, Google Changes Course, Signs Student Data Privacy Pledge, WSJ Blogs – Digits, January 20, 2015. <http://blogs.wsj.com/digits/2015/01/20/google-changes-course-signs-student-data-privacy-pledge/?mg=blogs-wsj&url=http%3A%2F%2Fblogs.wsj.com%2Fdigits%2F2015%2F01%2F20%2Fgoogle-changes-course-signs-student-data-privacy-pledge>.

301 See, e.g., Gry Hasselbalch, Privacy is the Latest Digital Media Business Model, Mediamocracy – Tech & Society, August 23, 2013. <http://mediamocracy.org/2013/08/23/privacy-is-becoming-a-digital-media-business-model-in-its-own-right-article-english-translation/>.

302 See, e.g., U.K. Info. Comm'r's Office, The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protections, 2010.

303 See Ann Cavoukian and Tyler J. Hamilton, The Privacy Payoff: How Successful Businesses Could Build Consumer Trust, 2002.

304 See Rubinstein (n. 198), (Noting that because some businesses «profit from targeted advertising, personalization, and price discrimination, they are strongly motivated to collect and analyze as much customer data as possible with the fewest possible restrictions.»)

Recent data for the US market suggests that user demand for privacy has indeed *increased* in the aftermath of the Snowden revelations. According to a recent survey by the Pew Research Center, 91% of surveyed adults agree or strongly agree that consumers have lost control over how personal information is collected and used by companies, and 64% say the government should do more to regulate what advertisers can do with their personal information.[305] Another Pew report shows that some users – largely in response to government surveillance programs – are shifting their basic behavior with technology: 30% of all adults have taken at least some steps to safeguard their privacy, for instance through changed privacy settings on social media, by reducing the use of social media, by avoiding certain apps, or by communicating more in person instead of online or on the phone.[306] While these reported changes in behavior are framed in terms of shielding information from the government, they suggest an increased overall demand for privacy in the digital environment, which directly affects companies that provide the platforms over which personal information is exchanged.

This group of privacy-aware users – the «privacy guardians» in contrast to the «information sellers» and «convenience seekers,» to use the typology by privacy scholar James P. Nehf[307] – is driving the demand for new business models in the market for privacy. While empirical evidence is currently not readily available, at least anecdotal evidence suggests the emergence of a vibrant *privacy startup scene* over the past few years.[308] While the lines between the different types of new companies are blurring, at least a few different approaches seem to emerge. Some startups are developing and marketing the next generation of (more) consumer-friendly privacy-enhancing technologies; several startups in Switzerland and Germany fall into this category.[309]

Others develop new business models for popular services such as search engines or social networking sites, which are no longer advertisement-based and hence are based on the collection and trade of users' personal information. Ex-

---

305 Madden (n. 147), pp. 37–38.

306 Lee Rainie and Mary Madden, Americans' Privacy Strategies Post-Snowden, Pew Research Center, March 16, 2015. <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>.

307 Nehf (n. 290), p. 14.

308 See, e.g., Making Sense of the Market for ‹pii' Products & Services | Privacy Identity Innovation, presented at the pii 2014 Conference, November 24, 2014. <https://www.privacyidentityinnovation.com/news/pii2014-making-sense-of-the-market-for-pii-products-services>; Julia Angwin and Emily Steel, Web's Hot New Commodity: Privacy, Wall Street Journal, February 28, 2011. <http://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

309 See, e.g., Michael J. Casey and Paul Vigna, BitBeat: Crypto Innovators Find Fertile Ground in Soft-Touch Switzerland, WSJ Blogs – MoneyBeat, August 4, 2014. <http://blogs.wsj.com/moneybeat/2014/08/04/bitbeat-crypto-innovators-find-fertile-ground-in-soft-touch-switzerland/>; Stephan Dörner, For German, Swiss Privacy Start-Ups, a Post-Snowden Boom, WSJ Blogs – Digits, August 20, 2014. <http://blogs.wsj.com/digits/2014/08/20/for-german-swiss-privacy-start-ups-a-post-snowden-boon/>.

ample includes DuckDuckGo, a search engine that does not collect or share personal information of its users;[310] Ello, a social networking site that distinguishes itself by promising to never sell user data to advertisers or third parties or show advertisements;[311] and the Swiss messaging app Threema, which saw a great influx of new users from Germany and Switzerland after Facebook acquired Whatsapp.[312] A different incarnation of services that target «privacy guardians» are services like Snapchat or Yik Yak, which address the peer-to-peer privacy dimension of the privacy challenge, for instance by deleting pictures after a certain period of time or allowing users to post anonymously.[313]

Other types of emerging business models are aimed at increasing user control over personal data at a more fundamental level by creating intermediary services that serve as trusted *data vaults* and as a negotiator between marketers who want access to its users' information. An example is Reputation.com, a company that offers a vault service to its users «by collecting data about consumers' marketing preferences and giving them the option to share that information on a limited basis with certain companies in exchange for coupons, say, or upgrades.»[314]

c. *Voluntary Self-Regulation*

As noted, a pure market model suggests that consumer preferences and transparency about companies' practices lead to an optimum level of privacy protection.[315] Although this «leave it to the market»[316] or laissez-faire approach is sometimes characterized as «self-regulation,»[317] the market model itself «make [s] no mention of self-regulation, and need[s] not rely on self-regulation in order to reach the desired privacy protection.»[318] From a theoretical perspective, self-regulation is a response to the observation that market «efforts to protect privacy are subject to significant limitations» and are seen as an alternative

---

310 See DuckDuckGo Privacy. DuckDuckGo, n.d. <https://duckduckgo.com/privacy>.

311 See Ello Privacy Policy. Ello, n.d. <https://ello.co/wtf/post/privacy>.

312 See Dominik Herrmann, Notwehr oder notwendiger Ungehorsam?, digma – Zeitschrift für Datenrecht und Informationssicherheit, pp. 150–154, 2014, p. 151 et seq.

313 Snapchat Privacy Policy, November 17, 2014. <https://www.snapchat.com/privacy>; Hannah Jane Parkinson, Yik Yak: The Anonymous App Taking US College Campuses by Storm, The Guardian, October 21, 2014. <http://www.theguardian.com/technology/2014/oct/21/yik-yak-anonymous-app-college-campus-whisper-secret>.

314 Natasha Singer, Company Envisions ‹Vaults' for Personal Data, The New York Times, December 8, 2012. <http://www.nytimes.com/2012/12/09/business/company-envisions-vaults-for-personal-data.html>.

315 See, e.g., Paul Rubin and Thomas Lenard, Privacy and the Commercial Use of Personal Information, New York 2002; Fred H. Cate, Privacy in Perspective, Washington, D.C. 2001.

316 See, e.g., Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? Seattle University Law Review, Vol. 34, No. 2, pp. 439–480, 2011, p. 455. <http://papers.ssrn.com/abstract=1758078>.

317 See, e.g., Solove (n. 289), pp. 70–81.

318 See Swire (n. 288), p. 6.

way to «create the reasonable protection of privacy without excessive cost.»[319] Nonetheless, at least certain forms of self-regulation in the privacy space, especially *voluntary* industry self-regulation, interact particularly closely with market realities (which is often mentioned as a particular advantage of this form of governance) and can arguably be subsumed under market-*based* approaches.[320]

As noted, self-regulation in the digital privacy context has a long tradition particularly in the US, dating back to the Clinton Administration's initial regulatory framework for electronic commerce and the Internet, in which it supported «private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution.»[321] Since the mid 90s, the FTC and other key agencies – with some important exceptions – have explicitly *promoted* a self-regulatory approach,[322] arguing «self-regulation can protect privacy in a more flexible and cost-effective manner than direct regulation without impeding the rapid pace of innovation in Internet-related businesses.»[323] More recently, consensus has seemed to emerge that self-regulation has not gone far enough and needs to be bolstered by legislation.[324]

European law- and policymakers have also acknowledged the role of self- and co-regulation for decades. Specifically, Article 27 (1) of the European Data Protection Directive encourages «the drawing up of codes of conduct intended to contribute to the proper implementation of national provisions [...], taking into account [...] the specific features of the various sections.» Similarly, Article 38 of the proposed General Data Protection Regulation states that Member States, data protection authorities, and the Commission «shall encourage the drawing up of codes of conduct [...], taking account of the specific features

---

319 See Swire (n. 288), p. 7. See also Hirsch (n. 316), p. 457.

320 See, e.g., Ira Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, I/S: A Journal of Law and Policy for the Information Society, Vol. 6, No. 3, pp. 355–423, 2011, p. 362. <http://papers.ssrn.com/abstract=1510275>; see also Solveig Singleton, Federal Standards for Internet Privacy: A Skeptical Approach, Cato Institute, July 13, 1999. <http://www.cato.org/publications/congressional-testimony/federal-standards-internet-privacy-skeptical-approach>; Damian Tambini, Danilo Leonardi and Chris Marsden, Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence, London and New York 2008. <https://www.suffolk.edu/documents/jhtl_book_reviews/Mastromauro08.pdf>. On the different notions of self-regulation, see, e.g., Weber (n. 14), pp. 22–24.

321 U.S. White House, Read the Framework: Global Information Infrastructure (GII), Whitehouse.gov, n.d. <http://clinton4.nara.gov/WH/New/Commerce/read.html>.

322 For an overview on FTC's evolving position on the self-regulatory approach to online privacy, see, e.g., Rubinstein (n. 320), pp. 364–367; Hoofnagle (n. 178), pp. 382–383.

323 See Rubinstein (n. 320), p. 356.

324 See, e.g., U.S. Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers, March 2012. <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

of the various data processing sectors [...].»[325] In addition to promoting self-regulation,[326] both the Directive and the proposed Regulation include detailed co-regulatory mechanisms.[327]

In the revision of the Data Protection Act in Switzerland, the Federal Council aims to strengthen self-regulation initiatives: industry organization, for instance, could phrase codes of good practice that would be sanctioned by the Federal Data Protection and Information Commissioner.[328] Such codes of good practice are also envisioned by some members of the advisory group for the revision of the DPA in order to add granularity to the law in the form of non-binding rules.[329]

The type of self-regulation (in addition to simply informing users about privacy practices through privacy policies)[330] that closest resembles the market-based approach is *voluntary* self-regulation where both norm-setting and enforcement are carried out by privacy firms or individual experts without any direct involvement of the government, often driven by the desire to prevent such involvement.[331] Both in the US and in Europe, a series of such initiatives have emerged, typically involving trade associations or firms «establishing substantive rules concerning the collection, use, and transfer of personal information, and procedures for applying these rules to member firms.»[332] Examples range from industry-wide efforts to develop common practices for online behavioral advertising across the Internet by a coalition of media and marketing trade associations,[333] to multi-stakeholder initiatives such as the Student Privacy Pledge[334] to safeguard student privacy based on commitments regarding the collection, maintenance, and use of students' personal information.[335]

---

325 See Article 38, Protection of Individuals with Regard to the Processing of Personal Data. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>.

326 An example of a pan-European voluntary self-regulatory standard is the IAB (Interactive Advertising Bureau) Europe's Self-Regulatory Framework for OBA and its supplementing EASA Best Practice Recommendation on Online Behavioral Advertising, see «EASA Best Practice Recommendations on Online Behavioral Advertising,» April 14, 2011. <http://www.easa-alliance.org/page.aspx/386>.

327 For an overview, see, e.g., Hirsch (n. 316), pp. 468–472.

328 See Schweizerischer Bundesrat (n. 231), p. 350.

329 Federal Office of Justice (n. 240), pp. 10–11.

330 See, e.g., U.S. Federal Trade Commission (FTC), Self-Regulation and Privacy Online: A Report to Congress, July 1, 1999. <https://www.hsdl.org/?view&did=744701>.

331 On the different types of self-regulation generally, see, e.g. Robert Baldwin, Martin Cave and Martin Lodge, Understanding Regulation: Theory, Strategy, and Practice, 2nd edition, New York 2013, pp. 39–41 and pp. 125–137; see also Weber (n. 14), pp. 22–32.

332 Rubinstein (n. 320), p. 356.

333 See, e.g., Self-Regulatory Program for Online Behavioral Advertising Factsheet. iab, n.d. <http://www.iab.net/media/file/OBA_OneSheet_Final.pdf>.

334 Student Privacy Pledge, Studentprivacypledge.org, n.d. <http://studentprivacypledge.org/>.

335 On the promise and limits of privacy multistakeholder processes, see Omer Tene and Trevor Hughes, The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study, Maine Law Review, Vol. 66, No. 2, pp. 437–465, 2014.

Another subtype of market-based approaches are *privacy seal programs* such as TRUSTe, BBBONline, ERSB Privacy Online Certification Seal, EuroPriSe, WebTrust, and CNIL, among others.[336] Recognized both in the US and Europe, privacy seal programs are «voluntary privacy measures adopted as a self-regulatory initiative to promote consumer trust and confidence in e-commerce. They enable organizations to demonstrate respect for privacy and develop a trustworthy image.»[337] Some of these programs play an important role not only with respect to voluntary regulation, but also in the context of government-endorsed self-regulation. Particularly, TRUSTe, the largest provider of privacy certifications globally, is an important participant in the EU-US Safe Harbor Framework, a US Children's Online Privacy Protection Act (COPPA) Safe Harbor certification provider, and the Accountability Agent for the US under the APEC Cross-Border Privacy Rules System.[338]

2. *Application*

a. *Big Data*

Anecdotal evidence suggests that privacy breaches that occur in Big Data environments *might* affect company's sales, damage its reputation, and influence its privacy policies and practices. For instance, after a massive data breach in 2013 including personal data of over 70 million consumers, the Target Corporation's profit declined over 40 percent within a quarter as a direct consequence of the incident.[339] After the same company used Big Data analysis to estimate when its female customers had become pregnant and personalize its sales strategy accordingly,[340] the company changed its privacy policy in response to negative media coverage and public opinion, indicating more clearly that it was using Big Data to personalize its marketing efforts, and allowing consumers to opt

---

336 See Rowena Rodrigues, David Barnard-Wills, David Wright, Paul De Hert and Vagelis Papakonstantinou, EU Privacy Seals Project: Inventory and Analysis of Privacy Certification Schemes – Final Report Study Deliverable 1.4. European Commission, 2013. <http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf>; Rowena Rodrigues, David Wright and Kush Wadhwa, Developing a Privacy Seal Scheme (that Works), International Data Privacy Law, May 5, 2013; Bhasin Dr. Madan Lal, Guarding Online Privacy: Privacy Seals and Government Regulations, European Journal of Business and Social Sciences, Vol. 1, No. 9, pp. 1–20, 2012. <http://www.ejbss.com/Data/Sites/1/decemberissue2012/ejbss-12–1179-guardingonlineprivacy.pdf>.

337 See Rodrigues/Barnard-Wills/Wright/De Hert/Papakonstantinou (n. 336), p. 10.

338 On the current crisis of TRUSTe, see Chris Connolly, Graham Greenleaf and Nigel Waters, Privacy Self-Regulation in Crisis? – TRUSTe's «Deceptive» Practices, December 1, 2014. <http://papers.ssrn.com/abstract=2567090>; and Rodrigues/Wright/Wadhwa (n. 336).

339 Elizabeth A. Harris, Data Breach Hurts Profit at Target, The New York Times, February 26, 2014. <http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?_r=0>. See also Target Reports Fourth Quarter and Full-Year 2013 Earnings, February 26, 2014. <http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678>.

340 See Duhigg (n. 51).

out.[341] Facebook, to take another example, had to withdraw changes in its privacy policy at least twice due to user protest and negative public reactions,[342] and also announced plans to improve its internal processes in the context of a recent mood manipulation experiment, which provoked very harsh reactions by the press and public.[343] Finally, Spanish telecommunications provider Telefónica was forced to backtrack from its announced plans to analyze and market localization data in Germany amid harsh criticism.[344]

With respect to *business model competition*, the previous section already mentioned the emergence of innovative services and applications that seek to compete with existing offerings on privacy grounds. While some of these services, such as Yik Yak and Snapchat, largely address privacy issues among their users (peer-to-peer privacy), other developments suggest competition among service providers in the Big Data business based on the data collection and usage practices. A recent example in this category is the YouTube Kids app, a video-streaming service for children launched by Google.[345] Unlike YouTube, the YouTube Kids app does not allow the collection or sharing of personal information. It cannot be linked to a Google account, nor can videos be uploaded or comments added to avoid the disclosure of personally identifiable information.[346] The competition between Microsoft's Outlook and Google's Gmail service is another illustration of how privacy features might be used as differentiators in the Big Data era, particularly in marketing campaigns.[347] More radical business model innovations in the Big Data marketplace designed with privacy in mind include services that provide «data vault» services and/or serve as interoperability platforms to both reduce vendor lock-in and increase user's control over data.[348] The Pro-

---

341 See, e.g., James R. Kalyvas and Michael R. Overly, Big Data: A Business and Legal Guide, Boca Raton 2014.

342 See, e.g., Brad Stone and Brian Stelter, Facebook Withdraws Changes in Data Use, The New York Times, February 19, 2009. <http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html>.

343 See, e.g., Robinson Meyer, Everything We Know About Facebook's Secret Mood Manipulation Experiment, The Atlantic, June 28, 2014. <http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>.

344 Heise Online, Telefónica: Keine Analyse von Bewegungsdaten in Deutschland, November 1, 2012. <http://www.heise.de/newsticker/meldung/Telefonica-Keine-Analyse-von-Bewegungsdaten-in-Deutschland-1741717.html>.

345 Introducing the Newest Member of Our Family, the YouTube Kids App – Available on Google Play and the App Store, Official YouTube Blog, n.d. <http://youtube-global.blogspot.com/2015/02/youtube-kids.html>.

346 See, e.g., Bill Shribman, YouTube's New Kids App: The Experts Weight In, Geek Dad, March 1, 2015. <http://geekdad.com/2015/03/youtubes-new-kids-app/>.

347 See, e.g., Russell Brandom, Microsoft Just Exposed Email's Ugliest Secret, The Verge, March 21, 2014. <http://www.theverge.com/2014/3/21/5533814/google-yahoo-apple-all-share-microsofts-troubling-email-privacy-policy>.

348 See, e.g. Omer Tene and Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, No. 239, pp. 263–270, 2013. <http://papers.ssrn.com/abstract=2149364>.

jectVRM, incubated at the Berkman Center for Internet & Society at Harvard University, is an example in this category.[349]

In addition to reputational effects and business model competition, voluntary self-regulation is a third type of a market-based approach addressed in this section that is very likely to shape future privacy policies and practices of companies in the Big Data business. First, many of the *self-regulatory frameworks* currently in place already affect companies' privacy policies and practices in Big Data environments. At the most basic level, the intra-firm standards established by big players such as Google, Microsoft, or Facebook will shape the level of privacy protection, as will existing industry self-regulation such as the best practice standards and recommendations in the field of Online Behavioral Advertising (OBA), which seek to regulate the delivery of ads to users based on their online activity, to name one prominent example.[350] In addition, new self-regulatory initiatives addressing specific privacy issues related to Big Data or dealing with certain applications are likely to emerge. The recently adopted standard ISO/IEC 27018:2014[351] governing the processing of personally identifiable information in public clouds – as a core Big Data infrastructure – might be seen as a precursor in this respect. As further discussed below, codes of conduct in the Big Data era are likely to play an increasingly important role particularly under the (enhanced) co-regulatory models envisioned both in the US and in Europe.

b. Internet of Things

Given its relatively nascent state of development, the application of market-based approaches to the privacy challenges associated with the Internet of Things is more speculative when compared to more mature markets. That being said, and considering standard economic theory,[352] it can be expected that consumer privacy preferences and reputational effects will also shape – to varying degrees – privacy policies and practices of companies that are part of the Inter-

---

349 See Project VRM. <https://cyber.law.harvard.edu/research/projectvrm>.

350 See, e.g., Daniel Castro, Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising, The Information Technology & Innovation Foundation, December 2011. <http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf; Clifford, Damian>; EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster – Tracking the Crumbs of Online User Behaviour, Journal of Intellectual Property, Information Technology, and Electronic Commerce Law, Vol. 5, No. 3, 2014. <http://www.jipitec.eu/issues/jipitec-5-3-2014/4095>.

351 Information Technology—Security Techniques—Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors, Standards Document. International Organization for Standardization, 2014. <http://www.iso.org/iso/catalogue_detail?csnumber=61498>. See, e.g., Paul De Hert, Vagelis Papakonstantinou and Irene Kamara, The New Cloud Computing ISO/IEC 27018 Standard through the Lens of the EU Legislation on Data Protection, Brussels Privacy Hub, November 2014. <http://www.brusselsprivacyhub.org/Resources/BPH-Working-Paper-VOL1-N 2.pdf>.

352 De Hert/Papakonstantinou/Kamara (n. 351).

net of Things ecosystem. As in other areas of application, the disciplining force of market-based mechanisms will depend on a number of variables. Perhaps more importantly, companies will face very different risks of negative reputation depending on the degree to which the core business model is based on the collection and use of personal information. While leading Internet of Things companies might share similar baseline incentives to avoid negative publicity, the risk of negative reputational effects are likely to be different whether, for instance, looking at a company that collects and processes data from sensors monitoring the performance of machine turbines, versus a company that places sensors into a person's home or measures every movement, tracking consumption patterns and allowing insights into life style habits, versus a company that uses EKG sensors with a patient's Smartphone to monitor and transmit vital signs and information about the physical environment to a health care provider.[353]

While it is too early to tell whether business model competition will be a relevant driver of optimal levels of privacy protection among Internet of Things companies as the relevant markets are still developing and the availability of alternative offerings is largely unknown, it seems safe to state that *self-regulation* is going to play an important role in the rapidly evolving Internet of Things ecosystem, which typically spans multiple jurisdictions.[354] A recent FTC Staff Report, for instance, «agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.»[355] An example is the Privacy Voluntary Code of Conduct, the outcome of a multistakeholder process facilitated by the United States Department of Energy's Office of Electricity Delivery and Energy Reliability and the Federal Smart Grid Task Force, which recommends high-level principles of conduct for both utility companies and third parties.[356]

Over the past years, voluntary self-regulation has been the dominant regulatory model in the Internet of Things, with ISO and EPCglobal as key *standard setting bodies*.[357] With respect to privacy self-regulation, the above-mentioned GS1 standards are illustrative:[358] In addition to the creation of a multi-industry,

---

353 For an overview of the top 10 industries investing in sensors, see Sensing the Future of the Internet of Things, Pricewaterhouse Coopers LLP, 2014. <http://www.pwc.com/us/en/increasing-it-effectiveness/assets/future-of-the-internet-of-things.pdf>. See also U.S. Federal Trade Commission (FTC) (n. 56), pp. 14–18.

354 Weber/Weber (n. 265), pp. 23–26. On the RFID standard development challenge more broadly, see, e.g., Harvey Lehpamer, Rfid Design Principles, 2nd edition, Norwood 2012, pp. 101–106.

355 U.S. Federal Trade Commission (FTC) (n. 56), p. 49.

356 See Voluntary Code of Conduct (VCC): Final Concepts and Principles, United States Department of Energy, January 12, 2015. <https://www.smartgrid.gov/sites/default/files/VCC_Concepts_and_Principles_2015_01_08_FINAL_1.pdf>.

357 See Weber (n. 43), p. 27.

358 See Standards Overview, GS1, December 20, 2014. <http://www.gs1.org/standards-overview>.

global Public Policy Steering Committee charged with anticipating and engaging in policy issues, GS1 members developed the Guidelines on EPC for Consumer Products,[359] «which promote consumer notice, education, and choice about the technology and include consumer privacy protections» as well as associated educational toolkits.[360]

The Guidelines emphasize the need for collaboration between manufacturers and retailers to provide clear notice to consumers so that they know the product they are purchasing contains an EPC tag.[361] Voluntary self-regulation – at least as a complement to an emerging legal framework – is likely to continue playing an important role, particularly vis-à-vis the technical and dynamic nature of the subject matter and given the difficulty of establishing uniform global legal norms.[362]

3. Evaluation

a. Promise

Market-based approaches to the contemporary digital privacy crisis are increasingly met with skepticism, including in the US, where self-regulatory schemes have dominated large parts of the consumer privacy landscape. The limits of the approach are discussed in the next section. Looking at the approach's promise, however, it is important to acknowledge at the outset that the market mechanisms discussed in the previous paragraphs are in fact at work and will continue to play an important role in the future. A separate question is to what extent market-based approaches will lead to an adequate level of privacy protection.

Depending on the specific market conditions and contexts, consumer preferences and reputational effects based on companies' privacy practices can at least in theory be efficient and highly dynamic mechanisms to deal with privacy issues that evolve so quickly in today's quicksilver technology environment. Going forward, *unlocking* the promise of such mechanisms in practice will require supporting strategies and interventions, such as user education and empowerment, including transparency tools and mechanisms, and depend on the level of market competition and the availability of alternative services and products. The survey data summarized above, the reports about some users' behavioral change with the goal to manage privacy risk exposure online, and the emergence of new, more privacy-respecting business models might be seen as a sign that such conditions are not entirely hypothetical, and that basic market

359 Guidelines on EPC for Consumer Products, Text. GS1, December 30, 2014. <http://www.gs1.org/guidelines-epc>.

360 See Apparel and General Merchandise – Commonly Asked RFID Questions: Dispelling Myths, GS1, September 30, 2014. <http://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?command=core_download&entryid=1433&PortalId=0&TabId=785>.

361 Guidelines on EPC for Consumer Products (n. 359).

362 Weber (n. 43), pp. 27–28.

mechanisms – despite the significant limitations discussed below – can and will play a role for certain segments and populations and in the context of a blended privacy governance model.

While privacy-based business model competition is nascent, it seems particularly promising as a *source of innovation*. As already noted in the introduction, the digital privacy crisis is a phenomenon that has been in no small part the result of economic drivers, which interact with other factors.[363] Within this economic context, the currently dominant advertising-based business model of large online service providers – from Google to Facebook – is one key source of the extensive data collection and usage practices.[364] As competition based on the same business model gets increasingly difficult due to strong network effects[365] and as we move towards the Internet of Things,[366] alternative business models, which might serve as the basis of a new generation of privacy-respecting online services, are likely to emerge that might not only affect firms' basic incentive structure to amass personal information, but also stimulate innovation in privacy technology and design and the adoption of such innovations.[367] The emergence of micro-payment systems using Bitcoin is an example in this category.[368]

The promise of market-based approaches in general and self-regulation in particular includes a relatively long list of *features*, including efficiency, flexibility, incentive for compliance, low implementation costs, and learnability, among others.[369] Especially where technical expertise is needed to address

---

363 See e.g., Alessandro Acquisti, Stefanos Gritzalis, Sabrina Di Vimercati, and Costos Lambrinoudakis (Eds.), Digital Privacy: Theory, Technologies, and Practices, Boca Raton 2007.

364 See Ethan Zuckerman, The Internet's Original Sin, The Atlantic, August 14, 2014. <http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/>.

365 Sai Prakash Iyer, Hariprasad Pichai and Thomas Kuruvilla, Primium – Business Models for a Privacy-Conscious World, Prism, 2014. <http://www.adlittle.com/downloads/tx_adlprism/Primium.pdf>.

366 See, e.g., Gordon Hui, How the Internet of Things Changes Business Models, Harvard Business Review, July 29, 2014. <https://hbr.org/2014/07/how-the-internet-of-things-changes-business-models>.

367 For a use case, see, e.g., Zhan Liu, Riccardo Bonazzi, Boris Fritscher and Yves Pigneur, Privacy-Friendly Business Models for Location-Based Mobile Service, J. Theor. Appl. Electron. Commer. Res. Vol. 6, No. 2, 2011. <http://www.scielo.cl/scielo.php?pid=S0718-18762011000200009&script=sci_arttext>; see also
Dimitris Gritzalis, Konstantinos Moulinos and Konstantinos Kostis, A Privacy-Enhancing e-Business Model Based on Infomediaries, Proceedings of the International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security, pp. 72–83, London 2001.

368 See, e.g., PwC, Digital Disruptor: How Bitcoin is Driving Digital Innovaiton in Entertainment, Media and Communications (EMC), Consumer Intelligence Series, February 7, 2014. <http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-consumer-intelligence-series-bitcoins-entertainment-media-communications.pdf>.

369 See, e.g., Weber (n. 14), p. 27.

complex privacy challenges in an increasingly globalized market environment with larger normative frameworks still in flux, self-regulation is a feasible approach. For such reasons, experts have acknowledged the future role of voluntary self-regulation for the Internet of Things.[370] Broader legislative developments both in the US and Europe, however, suggest that «regulated self-regulation» as a form of indirect state regulation and co-regulation are likely to play an increasingly prominent role in the age of Big Data, moving beyond what has been the focus of this section.[371] The White House Discussion Draft on a Consumer Privacy Bill of Rights Act of 2015, for instance, relies heavily on codes of conduct developed by diverse stakeholders as a way of flexible implementation of baseline protection for individual privacy in the commercial arena.[372] Companies adopting and complying with a code of conduct as approved by the FTC, would benefit from safe harbor protection in case of any suit or action brought under the Act. Similarly, the proposed General Data Protection Regulation endorses the development of codes of conduct that can be submitted for regulatory approval by the European Commission.[373]

With respect to *privacy seals programs*, the proposed Data Protection Regulation also indicates a shift towards new co-regulatory mechanisms by encouraging, «in particular at the European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors.»[374] The proposed Regulation empowers the Commission to specify the criteria and requirements for the data protection certification mechanisms,[375] and describes (in its amended version) the certification process leading up to a «European Data Protection Seal» by the supervisory authority in cooperation with the European Data Protection Board, during which the authority may accredit specialized third party auditors to carry out the auditing of the controller or processor on its behalf.[376] While a specific legal framework governing certification schemes and seals in Europe is missing, the envisioned process indicates that «the European policy position is shifting more in favour of a collaborative approach that draws in key stakeholders more actively (ie engaging both government and industry).»[377]

---

370 See, e.g. Weber/Weber (n. 265), p. 26.

371 On regulated self-regulation, see Wolfgang Schulz and Thorsten Held, Regulated Self-Regulation as a Form of Modern Government: A Comparative Analysis with Case Studies from Media and Telecommunications Law. Eastleigh 2004; see also Hirsch (n. 316).

372 See U.S. White House (n. 180), Sec. 301.

373 See Art. 38 of the proposed General Data Protection Regulation.

374 Art. 39(1) of the Proposed General Data Protection Regulation.

375 Art. 39(2).

376 Art. 39(1a-1i).

377 Rodrigues/Wright/Wadhwa (n. 336), p. 105; see also Tene/Hughes (n. 335), p. 447–448.

b. Limitations

A large literature spanning across multiple fields from behavioral economics to political studies have identified and discussed the limitations of different types of market-based approaches to information privacy. From this very rich and rapidly growing body of knowledge, the following selected pointers might be particularly relevant with respect to the market-based mechanisms outlined in this section.

With respect to basic market forces, a series of empirical studies examining user control of privacy online as indicated by functional features of commercial websites conclude that, «current marketplace practices inhibit the potential for user information or control over the use, collection, and retention of personal information.»[378] Many studies have highlighted the problem of *incomplete information and information asymmetries* between users and companies, a problem that was already mentioned in the introduction.[379] As a result of the ecosystem complexity discussed earlier, it is very difficult for users to have a clear knowledge of what data companies and others collect about them, and how the information is used and with what consequences.[380] Information asymmetries and other forms of incomplete information are not the only challenges in privacy decision-making. As noted before, empirical and theoretical research suggests that even with sufficient information, users «would be unable to process and act optimally on vast amounts of data,» largely due to «our innate bounded rationality [that] limits our ability to acquire, memorize and process all relevant information, and [...] makes us rely on simplified mental models, approximate strategies, and heuristics.»[381] The degree to which cues influence perceptions of privacy – ranging from observing other users revealing information to the availability of privacy controls, which both lead to more information disclosure – is one of many illustrative examples.[382]

Similar to basic market forces, reputational effects also have *limited influence* on firms' privacy practices, as a series of studies focused on data breaches and their effects on prices and brand reputation suggest. For instance, data breaches typically have very little effect on a company's market value.[383] In re-

---

378 See, e.g., Yong Jin Park, A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. Policy & Internet, Vol. 6, No. 4, pp. 360–376, December 1, 2014, p. 74. <http://onlinelibrary.wiley.com/doi/10.1002/1944-2866.POI375/abstract>.

379 See, e.g., Nehf (n. 290).

380 See, e.g., Acquisti/Brandimarte/Loewenstein (n. 151), p. 509.

381 Alessandro Acquisti and Jens Grossklags, Privacy and Rationality in Individual Decision Making, IEEE Security and Privacy, pp. 24–30, 2005, p. 25. <https://www.dtc.umn.edu/weis2004/acquisti.pdf>.

382 For an extensive review of the state of research, see Acquisti/Brandimarte/Loewenstein (n. 151).

383 Elena Kvochko and Rajiv Pant, Why Data Breaches Don't Hurt Stock Prices, Harvard Business Review, March 31, 2015. <https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices>.

cent years, stock prices of companies that experienced data breaches decreased only slightly and/or recovered very quickly after the event.[384] A 2012 study on the impact of 70 data breaches from 2004–2011 on share prices revealed that – on average – firms experienced a 0.1 % decrease in market value in response to such events.[385] In 33 of the cases, there was no measured effect on market returns.[386] Information asymmetries regarding privacy-relevant incidents and the difficulty of quantifying the longer-term effects of such events are among the reasons for these weak effects.[387] A sentiment-based event study, measuring the reputation effect of data breach incidents by analyzing users' reactions on social media platforms, shows a statistically significant short-term negative impact on a company's reputation within five days after the disclosure of the event.[388] While encouraging, any long-term effects remain unknown.

Business model competition, as noted above, is a potentially promising driver of more privacy protecting models as consumers demand increased protections surrounding their personal data. But there are various flaws to this approach, particularly to the extent that it is likely to lead to a situation where privacy protections only exist for those who can afford them. For example, a US company recently announced that users of its new fiber service can pay an additional $ 29/month to avoid being tracked by the provider.[389] While this is a clear price tag on privacy, an underlying difficulty of the relationship between users and data processing companies, as Preibusch notes, is that one consumer – in relation to Big Data (sets) – only produces small amounts of data and thus has little leverage to also benefit from the value generated through Big Data.[390] Thus, such a pay-for-privacy solution presents a very real problem for users who may value increased privacy protection, but cannot afford it – a situation particularly apparent when looking at the demographics of key social network-

384 Kvochko/Pant (n. 383).

385 Eric Helland and Jonathan Klick, The Market Impact of Privacy Breaches, December 6, 2012, p. 2. <http://www.masonlec.org/site/rte_uploads/files/Helland Klick privacy breaches 12 5 12.pdf>.

386 Helland/Klick (n. 385), p. 9. To take a recent example, though Target initially experienced a 10 % drop in stock prices following its holiday 2013 data breach of 70 million customers' personal information, by February 2014 Target's stock prices had experienced the largest percentage recovery in five years; Kvochko/Pant (n. 383).

387 Kvochko/Pant (n. 383).

388 Griselda Sinanaj, Jan Muntermann and Timo Cziesla, How Data Breaches Ruin Firm Reputation on Social Media! – Insights from a Sentiment-Based Event Study, in: Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik, 2015. <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1060&context=wi2015>.

389 Elizabeth Dwoskin and Thomas Gryta, AT&T Offers Data Privacy–for a Price, WSJ Blogs – Digits, February 18, 2015. <http://blogs.wsj.com/digits/2015/02/18/att-offers-data-privacy-for-a-price/?mod=WSJ_TechWSJD_NeedToKnow>.

390 Sören Preibusch, Big Data, Small Money, No Privacy?, digma – Zeitschrift für Datenrecht und Informationssicherheit, pp. 18–21, 2013, p. 20. <http://preibusch.de/publications/Preibusch__Big-Data_Value-of-Privacy_digma-2013.pdf>.

ing sites.[391] Another limiting factor here is a lack of trust by consumers: a recent survey from Germany shows that 61 percent of the Internet-users above the age of 14 are not willing to pay extra to be guaranteed that their data is only used as they wish and not utilized to generate other monetary value; of those who do not want to pay extra, 59 percent say that this is a result of their mistrust of data security.[392]

Similarly, *voluntary self-regulation* is not without (significant) limitations. There has been an emerging consensus among experts in recent years that voluntary privacy self-regulation has been largely unsuccessful. Generally, the effects of voluntary self-regulation are limited by two factors: first, many stakeholders will only participate in such efforts if it serves their own interest and, second, self-regulation is not legally binding and lacks enforcement mechanisms.[393] As a result, non-compliance does not necessarily lead to sanctions or adverse effects.[394] A 2011 report by the World Privacy Forum, for instance, describes the failure of a variety of self-regulatory privacy programs, including the BBBOnline Privacy Program mentioned earlier.[395] Insufficient oversight and enforcement, the significant profit to be gained by violating standards, and lack of penalties led to the failure of these – and other – voluntary self-regulatory regimes.[396] The FTC actions against TRUSTe – the world's largest provider of privacy seals, including to the three most important privacy self-regulatory schemes – and the recent settlement[397] is another example that illustrates the larger questions and limitations of self-regulatory approaches.[398] Concerns about the ineffectiveness of voluntary privacy self-regulation are not limited to the US, for instance as the evaluation of the European behavioral advertising voluntary code of conduct illustrates.[399]

---

391 According to a recent study by the Pew Research Center, 71 % of all adults online use Facebook, including 76 % of individuals making $ 30,000 or less per year (a higher percentage than the population at large), compared to 17 % of Twitter users. See Maeve Duggan, Nicole Ellison, Cliff Lampe, Amanda Lenhart and Mary Madden. Social Media Update 2014. Pew Research Center, January 9, 2015. <http://www.pewinternet.org/2015/01/09/demographics-of-key-social-networking-platforms-2/>.

392 Deutsches Institut für Sicherheit und Vertrauen im Internet, Daten – Ware und Währung, November 2014. <https://www.divsi.de/wp-content/uploads/2014/11/DIVSI-Studie-Daten-Ware-Waehrung.pdf>.

393 See, e.g., Weber/Weber (n. 265), p. 26.

394 Weber/Weber (n. 265), p. 26.

395 Robert Gellman and Pam Dixon, Many Failures: A Brief History of Privacy Self-Regulation in the United States, World Privacy Forum, October 14, 2011, p. 12. <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>.

396 Gellman/Dixon (n. 395), p. 27; see also Hoofnagle (n. 178), pp. 397–398.

397 U.S. Federal Trade Commission (FTC). TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program, November 17, 2014. <https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its>.

398 See, e.g., Chris Connolly, Graham Greenleaf and Nigel Waters, Privacy Self-Regulation in Crisis? – TRUSTe's «Deceptive» Practices, 132 Privacy Laws & Business International Report, Rochester, pp. 13–17, 2014. <http://papers.ssrn.com/abstract=2567090>.

399 Marc Rotenberg and David Jacobs, Updating the Law of Information Privacy: The New Framework of the European Union, Harvard Journal of Law and Public Policy, Vol. 36, No. 2,

4. *Outlook*

As already noted earlier, the importance of market forces – in addition to technological advancements – can hardly be underestimated when discussing the future of privacy in the digital age. Over the past decades, market forces have been instrumental in the making and shaping of today's digital privacy crisis, particularly through the advent of advertisement-based business models. This section has focused on the question as to what extent market forces might help, in the future, to address some of the challenges identified throughout this report. The answer to this question is *mixed*. While reputation and user demand will naturally continue to be important factors in a blended governance framework, their effects on companies' privacy practices are severely limited as a growing body of empirical and theoretical studies from various disciplines demonstrate. While some of these limits might be pushed – for instance through more effective intermediaries or by a next generation of tools that amplify relevant information about privacy practices for users – basic constraints such as information asymmetries and biases will remain.

Arguably more promising than the reliance on reputational effects are emerging business models that might lead the way to more privacy-respecting services. However, to what extent and for which demographics the next generation of business models will be able to address the digital privacy challenges of our time remains uncertain. That said, business model competition is likely to be an important element in the mix of approaches, particularly in its interaction with technological advancements and as an evolving source and driver of innovation. Similarly, self-regulatory approaches are likely to play a productive role moving forward. While privacy self-regulation in the incarnation of voluntary self-regulation has largely failed, the trend towards and experiences with «regulated self-regulation» in general and co-regulation in part seems particularly promising and worth supporting from a policy perspective.[400]

Taken together, the observations in this section suggest that the market-based approaches reviewed here are likely to be most promising when seen as part of a larger governance effort aimed at addressing digital privacy challenges. Against this backdrop and with respect to the future of digital privacy, it is important to overcome the traditional dichotomy between market-based solutions on the one hand and – where markets fail – government regulation on the other hand. Rather, market-based approaches can be *complementary* to and *supportive* of government-led regulation, and vice versa. From such a perspective of blended governance, it also becomes clear that the role of law when shaping the future of privacy is significantly broader than what traditional accounts that focus on information privacy or data protection law indicate, and

---

pp. 627–652, 2013. <http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf>.

400 See also RUBINSTEIN (n. 320).

may include areas such as competition law and procurement law, to name just two examples. Similarly, the role of governments in the privacy context has to be re-envisioned and expanded beyond the (traditional) role of the regulator, as further discussed below.[401]

IV. Human-Centered Approaches

1. Approach

a. Awareness, Education, and Digital Literacy

Over the past decade, privacy experts have emphasized the importance of equipping users with the necessary means to both understand and successfully deal with the multi-faceted digital privacy challenges of our time. At the most basic level, awareness-raising and educational efforts have been identified as strategies to empower users to protect their privacy. Such *information-based approaches* are often characterized as «the first line of defense in ongoing efforts to better protect privacy in the information age,»[402] and are conceptually aimed at leveling information asymmetries between the different actors, and/or seen as approaches to overcome some of the cognitive limitations of users when making decisions about the disclosure of personal information.[403] Philosophically, awareness-building and education-based approaches are linked to concepts of self-responsibility «by incentivizing users to be more vigilant about protecting their own privacy,»[404] but do «not necessarily mean governments have no role to play.»[405]

Awareness-building and educational efforts concerning digital privacy have a long tradition and involve many different actors. Governments around the world are heavily engaged in explaining privacy risks to users, and offer strategies and tips for both individuals and companies. The FTC, for instance, stipulates as a principle in its seminal report on consumer privacy protection in the digital age that «[a]ll stakeholders should expand their efforts to educate consumers about commercial data privacy practices.»[406] The European Commission, to take another example, also highlights the role of awareness-

401 Gasser/O'Brien (n. 162).

402 Adam Thierer, The Pursuit of Privacy in a World Where Information Control Is Failing, Harvard Journal of Law and Public Policy, Vol. 36, No. 2, pp. 410–455, 2013, p. 437. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680>.

403 See generally Howard Beales, Richard Craswell and Steven Salop, The Efficient Regulation of Consumer Information, Journal of Law and Economics, Vol. 24, No. 3, pp. 491–539, 1981. <http://chicagounbound.uchicago.edu/jle/vol24/iss3/10/>.

404 Adam D. Thierer, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, George Mason Law Review, Vol. 20, No. 4, pp. 1055–1105, 2013, p. 1092. <http://papers.ssrn.com/abstract=2309995>.

405 Thierer (n. 402), p. 1092.

406 U.S. Federal Trade Commission (FTC) (n. 56), p. 72.

raising and user education as part of the general objectives of consumer protection,[407] and its recent synthesis report on consumer policy emphasizes the importance of such information-based strategies as a means to empower consumers.[408] In Switzerland, the need for awareness-raising and education on privacy is further emphasized by the authors of the report on the evaluation of the Data Protection Act, who have remarked that expert interviews and surveys of the population reveal diverging opinions regarding the people's ability to correctly assess the (technological) possibilities of data processing.[409] In its Social Media Report, the Federal Council responds to a parliamentary postulate regarding the Swiss legal framework for Social Networking Sites and the necessity for possible changes thereof in order to close loopholes. The Federal Council's Report favors an approach of information sharing and awareness raising rather than regulation (while the review of the Data Protection Act is still in progress), noting that optimal results will only be achieved by also applying extralegal measures.[410] The Federal Council further remarks that fostering media literacy among children and youth – as well as educators and caretakers – is key.[411]

Government agencies have not only promoted user awareness and education as a first line of defense against privacy invasion in high-level policy reports and statements, but have also engaged in a wide range of information-based activities at the implementation level. According to one study, data protection authorities across Europe «have become increasingly involved in policy issues, guidance, advice, education, awareness-raising and a host of other activities that present opportunities for creating a ‹privacy culture' alongside, and possible helping to control and guide, the ‹information society›.»[412] As part of the Consumer Agenda, the European Commission launched a community website for consumer education with a broad range of teaching materials, including resources on digital literacy and new media.[413] Along similar lines, the FTC

---

407 See, e.g., European Commission, A European Consumer Agenda – Boosting Confidence and Growth, May 5, 2012. <http://ec.europa.eu/consumers/archive/strategy/docs/consumer_agenda_2012_en.pdf>.

408 European Commission, Report on Consumer Policy, 26–31, January 2012–December 2013. <http://ec.europa.eu/consumers/strategy-programme/policy-strategy/documents/consumer_policy_report_2014_en.pdf>.

409 Buro Vatter, Christian Bolliger and Marius Feraud, Evaluation des Bundesgesetzes über den Datenschutz, Institut für Europarecht, Universität Freiburg, March 10, 2011, p. 66.

410 Federal Council, Rechtliche Basis für Social Media – Bericht des Bundesrates in Erfüllung des Postulats Amherd, 11.3912, September 29, 2011, p. 75. <http://www.bakom.admin.ch/themen/infosociety/04837/index.html?lang=de&download=NHzLpZeg7 t,lnp6I0NTU042l2Z6ln1acy4Zn4Z 2qZpnO2Yuq2Z 6gpJCDfH59fWym162epYbg2c_JjKbNoKSn6A–>.

411 Federal Council (n. 410), 76.

412 European Commission, Evaluation of the Means Used by National Data Protection Supervisory Authorities in the Promotion of Personal Data Protection, 2007, p. 2. <http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_kantor_management_consultants.pdf>.

413 See also European Commission, Consumer Classroom. <http://www.consumerclassroom.eu>.

teamed up with other federal agencies to offer OnGuardOnline,[414] a website with safety and privacy tips for consumers and businesses – among a long list of other awareness-raising and educational efforts.[415]

In Switzerland, the Federal Council's Strategy for a Policy for Children and Youth from 2008, with regard to Internet usage, focused mostly on online safety and exposure to violence.[416] Yet, following a report on youth and violence prevention from 2009, the Federal Department of Home Affairs was instructed to create a program for the protection of youth in media and media literacy.[417] While privacy was not the main focus of the resultant document, it was therein pointed out that self-regulation regarding data protection – especially of social networking sites – had not been well developed at that time.[418] The program takes a broad approach to fostering (digital) media literacy of children and youth. For instance, it creates a common platform for existing offerings for awareness-raising, seeks to strengthen the continued development and quality assurance of (educational) materials, and drives the development and testing of innovative strategies and projects to reach at-risk persons.[419] In this program – Youth and Media («Jugend und Medien») – Government agencies collaborate with the private sector on a variety of areas, such as sponsoring research projects that analyze the use of online media by children and youth in Switzerland.[420]

Initiatives aimed at educating users about privacy challenges and ways to preserve privacy in the digitally networked environment often also emerge in a bottom-up fashion and are led by the private sector. Particularly in developing countries, Western technology companies play an important role in educating the educators – parents and teachers – as well as young users about safety and privacy risks online.[421] In the US and in Europe companies have also shown

---

414 OnGuardOnline, <https://www.onguardonline.gov>.

415 See, e.g., Thierer (n. 402), p. 439.

416 Federal Council, Bundesrat, Strategie für eine schweizerische Kinder- und Jugendpolitik, August 27, 2008, p. 4 and p. 8. <http://www.bsv.admin.ch/aktuell/medien/00120/index.html?lang=de&msg-id=20941>.

417 See Bundesamt für Sozialversicherungen, Nationales Programm Jugendmedienschutz und Medienkompetenzen, June 11, 2010, p. 4. <http://www.jugendundmedien.ch/fileadmin/user_upload/Jugendschutz/Deutsch/100611_Nationales_Programm_Jugendmedienschutz_d.pdf>.

418 Bundesamt für Sozialversicherungen (n. 417), p. 7.

419 Bundesamt für Sozialversicherungen (n. 417), p. 14.

420 See the bi-annual JAMES studies by a research team at Zurich University of Applied Sciences and a report on trends in usage of digital media: Sarah Genner, Entwicklungs- und Nutzungstrends im Bereich der Digitalen Medien und damit verbundene Herausforderungen für den Jugendmedienschutz (Teilbericht I), 2013; Stephan Dreyer, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen für den Jugendmedienschutz (Teilbericht II), 2013. <http://www.jugendundmedien.ch/fachwissen/publikationen.html>.

421 A leading example is Yahoo!'s engagement in Vietnam, see UNICEF Media Center, Yahoo! Safely' Launched To Help Create a Safer Internet Environment For Users in Viet Nam, n.d. <http://www.unicef.org/vietnam/media_16185.html>.

that they can be effective facilitators of digital citizenship and digital literacy.[422] In addition, a significant number of non-profit organizations provide educational resources for users with an interest in privacy issues. Such offerings map on a spectrum from simple tips and recommendations on one end,[423] to rather sophisticated privacy rights clearinghouses on the other.[424] Some resources are relatively generic; others focus on specific issues, such as privacy on social networking sites. Similarly, some educational efforts are aimed at a general interest audience,[425] while others target specific audiences such as professionals, researchers, and the like.[426] Resources often include information in text form, but also video content, games, cartoons, and apps.[427] Some of the most advanced systems are code-based and rate and label privacy policies,[428] or track privacy policy changes over time.[429]

Not surprisingly, *children and young users* – typically considered a particularly vulnerable population – have frequently been the focus of educational efforts.[430] Around the globe, governments, international organizations, companies, NGOs, and privacy advocates have made a great variety of resources available to parents and other caregivers who play a key role in raising privacy awareness and promoting digital literacy, especially among younger chil-

---

422 See, e.g., Trustworthy Computing Initiative, Microsoft. <http://www.microsoft.com/en-us/twc/>; Yahoo! Privacy Center, Yahoo! <http://info.yahoo.com/privacy/us/yahoo>; Privacy Policy, Google. <http://www.google.com/privacy>. See also Adam Thierer, Public Interest Comment on U.S. Federal Trade Commission (FTC) Report, Protecting Consumer Privacy in an Era of Rapid Change, Mercatus Center at George Mason University, 2011, p. 9. <http://mercatus.org/sites/default/files/public-interest-comment-on-protecting-consumer-privacy-do-not-track -proceeding.pdf>.

423 See, e.g., Privacy and Internet Safety. <https://www.commonsensemedia.org/privacy-and-internet-safety>.

424 See, e.g., Privacy Rights Clearinghouse. <https://www.privacyrights.org/>.

425 See, e.g., Common Sense Media, Privacy and Internet Safety. <https://www.commonsensemedia.org/privacy-and-internet-safety>.

426 See, e.g., Berkman Center for Internet & Society, Privacy Tools for Sharing Research Data. <http://cyber.law.harvard.edu/research/privacy_tools>.

427 For video content, see, e.g. Your Digital Footprint – Leaving a Mark, Teaching Ditigal Citizenship, n.d. <http://www.teachinctrl.org/lessons/yourdigitalfootprint.php>. For games, see, e.g Privacy Playground: The First Adventure of the Three CyberPigs, Media Smarts, n.d. <http://mediasmarts.ca/game/privacy-playground-first-adventure-three-cyberpigs>. For cartoons, see, e.g., The Adventures of Super Peif, n.d. <http://comics.superpeif.com/index_en.html>. For apps, see, e.g., Wickr, a Mobile Privacy Application, Sweeps Digital Crumbs Away. PCWorld, July 27, 2012. <http://www.pcworld.com/article/258495/wickr_a_mobile_privacy_application_sweeps_digital_crumbs_away.html>.

428 See, e.g., Terms of Service; Didn't Read. <https://tosdr.org/>.

429 See, e.g., ToSBack2. The Internet Society and the Electronic Frontier Foundation. <https://tid.isoc.org/confluence/display/TOSBACK2/ToSBack2+Home>.

430 See generally Palfrey and Gasser (n. 137); Children's Online Privacy. Common Sense Media. <https://www.commonsensemedia.org/advocacy/childrens-online-privacy>.
Emma Brown, Obama to Propose New Student Privacy Legislation, The Washington Post, January 18, 2015. <http://www.washingtonpost.com/local/education/obama-to-propose-new-student-privacy-legislation/2015/01/18/2ad6a8ae-9d92–11e4-bcfb-059ec7a93ddc_story.html>. See also James (n. 133), pp. 23–46.

dren.[431] A number of initiatives have developed curriculums covering privacy and related issues that are sometimes aggregated under the header «digital citizenship.»[432] Others have focused on the development of peer-teaching and peer-learning modules that can be used in the classroom, but also in out-of-school settings and informal learning environments.[433]

As education itself lies within the competence of Cantons in Switzerland, the Swiss Conference of Cantonal Ministers of Education (EDK) has issued a strategy for ICT and media, which also emphasizes the importance of ICT literacy for children and youth. The EDK's strategy adopted in 2007 does not address privacy in particular, but recommends that educators be familiar with the relevant provisions of the Data Protection Act.[434] Moreover, in a move to harmonize education schedules for Kindergarten through 9th grade, the German speaking Cantonal Ministers of Educations have developed a common curriculum (carrying out a constitutional mandate) in the so-called «Lehrplan 21,» which includes goals for media and ICT literacy of students, for instance to know basic rules of security for their own data and to be aware of the effects of publishing their own content,[435] as well as of the risks of transmitting or storing data without encryption.[436]

The afore-mentioned EDK is also among three public bodies sponsoring Educa.ch, a national contact point for questions concerning ICT in education, which has published a guide on privacy in school.[437] In addition, Swiss Crime Prevention has published a brochure that gives guidance on safe behavior in social media called «My Little Safebook» (in separate versions for parents and

---

431 See, e.g, MEDIENKOMPETENZ: Tipps zum Sicheren Umgang mit Digitalen Medien, Jugend und Medien, January 2013. <http://www.jugendundmedien.ch/fileadmin/user_upload/Chancen_und_Gefahren/Broschuere_FAQ_Medienkompetenz_dt.pdf>.

432 See, e.g., Digital Literacy & Citizenship Classroom Curriculum. Common Sense Media. <https://www.commonsensemedia.org/educators/curriculum>; Digital Literacy and Citizenship Curriculum. Google. <https://www.google.com/goodtoknow/web/curriculum/>; 3 Ways to Weave Digital Citizenship into Your Curriculum. International Society for Technology in Education, March 15, 2014. <https://www.iste.org/explore/articleDetail?articleid=50&category=ISTE-Connects-blog&article=3-ways-to-weave-digital-citizenship-into-your-curriculum>.

433 See, e.g., Catherine Cronin, Students, Peer Learning, and Google+. Catherinecronin, November 4, 2011. <https://catherinecronin.wordpress.com/2011/11/04/students-google-and-collaborative-learning/>; see also Youth and Media. Berkman Center for Internet & Society. <http://www.youthandmedia.org>.

434 EDK, Empfehlungen für die Grundausbildung und Weiterbildung der Lehrpersonen an der Volksschule und der Sekundarstufe II im Bereich der Informations- und Kommunikationstechnologien ICT, March 25, 2004, p. 9. <http://edudoc.ch/record/24707/files/Empf_ICT_LB_d.pdf>.

435 See Lehrplan 21 Module MI.1.3. <http://vorlage.lehrplan.ch/index.php?nav=200|41&code=a|10|0|1|0|3>.

436 See Lehrplan 21 Module MI.2.3. <http://vorlage.lehrplan.ch/index.php?nav=200|42&code=a|10|0|2|0|3>.

437 See Schule, ICT und Datenschutz. Educa, 2009. <http://guides.educa.ch/sites/default/files/schule_ict_und_datenschutz_d_0.pdf>.

children).[438] The brochure mostly addresses risks and dangers such as cyberbullying, molestation, and pornography but also evokes the importance of «data frugality» online. Other Swiss examples of initiatives that seek to educate about privacy include NetLa and ThinkData. The former, under patronage of the Federal Data Protection and Information Commissioner, seeks to teach children between the ages of 5 and 14 about the importance of privacy online through games and quizzes.[439] The latter is a joint initiative by data protection researchers and officers to raise awareness for issues of data processing (and transparency) in organizations.[440] ThinkData provides an FAQ and certain real-life scenarios to guide privacy decisions.

Closely related to information-based strategies such as awareness-raising and education is the approach of empowering users via *digital self-help tools* and privacy-enhancing technologies (PETs). The concept of PETs is discussed in greater detail in an earlier section of this report. A wide variety of such tools and strategies aimed at protecting user privacy are available on the marketplace today, ranging from ad preference managers to reputation protection services.[441] However, as noted before, this diverse arsenal of safety and privacy tools has not been widely adopted by users. Some commentators suggest that this lack of adoption might be grounded in the lack of awareness among users, and that governments and other actors can «take steps to encourage the use of such tools and methods, such as developing their own websites, online tools, and even privacy-enhancing applications in order to further empower citizens.»[442] In contrast, other scholars argue that «this lack of awareness reflects information asymmetries and that this and related market failures are difficult to correct absent regulatory intervention.»[443]

b. Improving Choice Architecture («Soft Paternalism»)

Building awareness of privacy challenges in users, increasing their level of education about risks and preventive strategies, and empowering consumers through tools to handle privacy issues in their chosen manner are core elements

438 My Little Safebook, Schweizerische Kriminalprävention, January 2013. <http://news.skppsc.ch/2013/01/24/neue-broschure-my-little-safebook-fur-einen-sicheren-umgang-mit-den-sozialen-medien/>.

439 NetLa. <http://www.netla.ch/>.

440 Think Data, n.d. <http://www.thinkdata.ch/>. The Federal Data Protection and Information Commissioner's office is among several independent bodies involved in this initiative.

441 For an overview, see, e.g., THIERER (n. 402), pp. 440–446.

442 THIERER (n. 404), p. 1097.

443 See, e.g., RUBINSTEIN (n. 198), p. 1432; see also SOLOVE (n. 289), pp. 76–92; JERRY KANG, Information Privacy in Cyberspace Transactions, Stanford Law Review, Vol. 50, pp. 1193–1294, 1998. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=631723>; PAUL M. SCHWARTZ, Property, Privacy, and Personal Data, Harvard Law Review, Vol. 117, No. 7, pp. 2076–2084, May 2004. <http://papers.ssrn.com/abstract=721642>. See THIERER (n. 404), p. 1097 (footnote 277) for opposing views.

of what one might call a «human-centered» approach to the digital privacy challenge. Another important component focuses on the social, psychological, and emotional parameters and components of user behavior when seeking to confront privacy challenges, and aims «to influence choices in a way that will make choosers better off, as judged by themselves.»[444] In essence, this approach takes into account a growing body of research mostly from the field of *behavioral economics* that studies how users make privacy decisions, [445] and explores how individual choices can be improved through system design to increase individual and social welfare.[446]

As noted earlier in this report, privacy decisions are often complex and sometimes overwhelming in the sense that «the cognitive costs associated with considering all the ramifications of a disclosure may hamper decision making.»[447] Further, users have to make decisions about the disclosure of personal data and other privacy-relevant choices under *conditions of uncertainty*, where users might face information asymmetries and therefore not have full knowledge about the relevant data collection and usage practices. In addition, findings from behavioral economics and behavioral decision research demonstrate how users are affected by a series of *cognitive and behavioral biases* when making privacy-relevant choices.[448]

Building upon the general idea of *nudging* – popularized by Richard Thaler and Cass Sunstein – as a form of «soft paternalism» to influence and improve decision-making in situations where such biases may adversely affect users, there has been a growing interest in the application of this concept in the context of privacy. Nudge is defined as «any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives.»[449] The use of privacy nudges

---

444 Richard Thaler and Cass Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness, New York 2009, p. 5.

445 For a general discussion of potential behavior approaches, see FJ Zuiderveen Borgesius, Consent to Behavioural Targeting in European Law – What Are the Policy Implications of Insights from Behavioural Economics?, Amsterdam Law School Research Paper No. 2013-43. <http://papers.ssrn.com/abstract=2300969>.

446 Alessandro Acquisti, Nudging Privacy, The Behavioral Economics of Personal Information, IEEE Security and Privacy, Vol. 7, No. 6, pp. 82–85, 2009; see also Anthony Jameson, Bettina Berendt, Federica Cena, Fabiana Vernero, Silvia Gabrielli, Christina Gena and Katharina Reinecke, Choice Architecture for Human-Computer Interaction, Vol. 7, No. 1–2, pp. 1–235, 2013.

447 Rebecca Balebako, Pedro G. Leon, Hazim Almuhimedi, Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Faith Cranor and Norman Sadeh, Nudging Users Towards Privacy on Mobile Devices, 2011, p. 1. <http://ceur-ws.org/Vol-722/paper6.pdf>.

448 Balebako/Leon/Almuhimedi/Kelley/Mugan/Acquisti/Cranor/Sadeh (n. 447); see also, Somini Sengupta, Web Privacy, and How Consumers Let Down Their Guard, The New York Times, March 30, 2013. <http://www.nytimes.com/2013/03/31/technology/web-privacy-and-how-consumers-let-down-their-guard.html>.

449 Thaler/Sunstein (n. 444), p. 4.

as a means to nudge (instead of force) people towards more thoughtful and better-informed privacy-relevant decisions was pioneered by Alessandro Acquisti and has recently received increased attention by policymakers as well as technology designers.[450]

While privacy nudge theory and practice is still in relatively early phases, privacy researchers have started to engage in a series of exploratory studies and field trials, using various types of nudging interventions. Privacy nudges have been developed and used in the context of social networking sites,[451] but also applied to mobile devices and applications.[452] These studies demonstrate how technology designers could apply the nudging approach to improve users' decision-making with respect to privacy. Here, soft paternalism connects with some of the concepts introduced in the privacy by design section of this report. It is important to realize that such nudges are not entirely new and have already been deployed by industry players over several years – mostly, however, to encourage users to reveal and share *more* personal information, not less.[453] The industry's strategic (or perhaps more accurately: biased) use of defaults – a particularly powerful nudge[454] – in the context of the privacy settings of social media sites in order to maximize information sharing is particularly illustrative in this respect.[455]

Thaler and Sunstein discuss the soft paternalistic approach in the context of public policy and examine how governments can use «nudging» to achieve particular policy goals. And indeed, the nudge concept has gained traction among policymakers in a broad range of fields ranging from prevention of securities

---

450 See Acquisti (n. 446), pp. 82–85.

451 See, e.g., Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti and Lorrie Faith Cranor, Privacy Nudges for Social Media: An Exploratory Facebook Study, in: Proceeding WWW '13 Companion, pp. 763–770, 2013. <https://www.andrew.cmu.edu/user/pgl/psosm2013.pdf>; Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget and Norman Sadeh, A Field Trial of Privacy Nudges for Facebook, 2014. <http://yangwang.syr.edu/papers/CHI2014.pdf>; Yang Wang, Pedro Giovanni Leon, Xiaoxuan Chen, Saranga Komanduri, Gregory Norcie, Kevin Scott, Alessandro Acquisti, Lorrie Faith Cranor and Norman Sadeh, From Facebook Regrets to Facebook Privacy Nudges, Ohio State Law Journal, Vol. 74, No. 6, pp. 1307–1334, 2013. <http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/19-Wang-Leon-Chen-Komanduri-Norcie-Scott-Acquisti-Cranor-Sadeh.pdf>.

452 Balebako/Leon/Almuhimedi/Kelley/Mugan/Acquisti/Cranor/Sadeh (n. 447).

453 See, e.g., Balebako/Leon/Almuhimedi/Kelley/Mugan/Acquisti/Cranor/Sadeh (n. 447), p. 2.

454 See, e.g., Cass Sunstein, Deciding By Default, University of Pennsylvania Law Review, Vol. 162, No. 1, pp. 1–57, 2013. <http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn_law_review>.

455 See, e.g., Jef Ausloos, Els Kindt, Eva Lievens, Peggy Valcke, and Jos Dumortier, Guidelines for Privacy-Friendly Default Settings, ICRI Research Paper No. 12/2013, February 18, 2013. <http://papers.ssrn.com/abstract=2220454>; Rony Hirshpung, Hadas Shwartzh-Chassidim, and Eran Toch, An Algorithmic Approach To Evaluating Default Privacy Options, 2014 TPRC Conference Paper, March 31, 2014. <http://papers.ssrn.com/abstract=2418596>.

fraud to environmental law.[456] With respect to privacy, insights from behavioral research may not have yet translated into advanced «nudging» legislation, but have certainly informed policy debates. In Europe, for instance, the change from an opt-out to an opt-in design governing the use of cookies according to the E-Privacy Directive was influenced by behavioral considerations.[457] More broadly, the importance of defaults as a «nudge» has been widely acknowledged in policy debates about privacy on both sides of the Atlantic – often discussed under the header «Privacy by Default.»[458] The FTC, for instance, advocates that social networking sites «should consider implementing more privacy-protective default settings for teens,» which could at least function as speed bumps.[459] Similarly and also in the context of social networking sites, the Article 29 Data Protection Working Party (to take a European example) highlighted the importance of privacy-friendly default settings.[460]

While the Swiss Federal Data Protection and Information Commissioner believes that well-informed people will make the right decisions, he also notes that the speed with which technology develops is a challenge.[461] To address this, he has suggested that Privacy by Default – among other approaches – be considered in the review of the Data Protection Act.[462] Privacy by Default, which in a way represents a «reversal of the privacy logic in favor of users,»[463] has also been put forward in the evaluation of the Data Protection Act[464] and is in accordance with the Federal Council's goals for the ongoing review of the Act[465] as well as part of the Swiss Government's Strategy for an Information

---

456 See, e.g, Tori DeAngelis, Coaxing Better Behavior, Monitor on Psychology, Vol. 45, No. 11, p. 62, 2014. <http://www.apa.org/monitor/2014/12/cover-coaxing.aspx>.

457 Alberto Alemanno and Alessandro Spina, Nudging Legally On the Checks and Balances of Behavioural Regulation, The Jean Monnet Center for International and Regional Economic Law & Studies, June 2013, p. 19. <http://www.jeanmonnetprogram.org/papers/13/documents/JMWP06AlemannoandSpina.pdf>.

458 For a critical assessment, see Lauren E. Willis, Why Not Privacy by Default?, Berkeley Technology Law Journal, Vol. 29, No. 1, 2014. <http://papers.ssrn.com/abstract=2349766>.

459 U.S. Federal Trade Commission (FTC) (n. 56), p. 60.

460 Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, Adopted June 12, 2009, p. 7. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf>.

461 Datenschutz ist kein Luxusgut, Neue Zürcher Zeitung, January 28, 2015. <http://www.nzz.ch/schweiz/datenschutz-ist-kein-luxusgut-1.18471125>.

462 See Thür, (n. 81), p. 96.

463 See Jean Christophe Schwaab, Privacy by Design/by Default – Inverser la logique de protection des données en faveur des utilisateurs. <http://www.schwaab.ch/archives/2013/09/26/privacy-by-design-by-default-inverser-la-logique-de-protection-des-donnees-en-faveur-des-utilisateurs/>.

464 Bolliger/Féraud/Epiney/Haenni (n. 63), p. 225.

465 Note that the Federal Council's report on the evaluation of the Data Protection Act talks about early effects of privacy law («frühes Greifen»), see Schweizerischer Bundesrat (n. 231), p. 350. Moreover, the Federal Council has recommended that the National Council adopt a postulate by Councillor Jean Christophe Schwab from September 23, 2013, which would mandate that the Government examine whether it would be practical to introduce privacy by default into

Society, which seeks to create the necessary preconditions to design products and services in a privacy-friendly way, and to give users corresponding default settings.[466]

2. *Application*

a. *Big Data*

Governments on both sides of the Atlantic have identified awareness-raising and user education as important elements of a multi-pronged strategy aimed at dealing with the privacy and data protection challenges related to Big Data. The White House report on Big Data, for instance, suggests that the federal government's consumer protection and technology agencies should convene a series of public workshops and issue reports to build *public awareness* about some of the privacy-related challenges of Big Data technologies.[467] Similarly, the role of consumer awareness in the age of Big Data with respect to specific data protection challenges such as data anonymization has been highlighted by the European Commission as part of its new strategy on Big Data, which seeks to support the transition towards a data-driven economy in Europe.[468]

Education and empowerment of young users has also been recognized in the Big Data context. For instance, the US government has launched a series of initiatives to encourage and enhance *digital literacy* and empower students to protect their privacy in the Big Data age.[469] The Swiss federal government, to take another example, launched a national program on youth, media, and literacy in 2010, which is aimed at educating children and youth about opportunities and risks online, including in Big Data environments such as social media sites.[470] The web portal of the initiative provides not only information, but also tools and resources to support parents, teachers, and schools in their efforts to encourage and build digital literacy among young users.[471] Media literacy education – including lessons about the function of algorithms – is also the (controversial) subject of a major overhaul of the Swiss public school curriculum.[472]

---

the Swiss data protection law, see <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133806>.

466 OFCOM, Strategy for an Information Society in Switzerland, Federal Council, p. 9. <http://www.bakom.admin.ch/themen/infosociety/04833/04834/index.html?lang=en>.

467 Executive Office of the President of the United States (n. 56), pp. 51–52.

468 See, e.g., European Commission, Making the Most of the Data-Driven Economy, July 2, 2014. <http://europa.eu/rapid/press-release_MEMO-14–455_en.htm>.

469 Executive Office of the President of the United States (n. 56), p. 52.

470 See Bundesrat, Nationales Programm Jugendmedienschutz und Medienkompetenzen, November 6, 2010. <http://www.news.admin.ch/NSBSubscriber/message/attachments/19468.pdf>.

471 See <http://www.jugendundmedien.ch/>.

472 See Lehrplan 21, Importance and Goals of the module Media and ICT. <http://vorlage.lehrplan.ch/index.php?nav=200|10&code=e|10|1>.

Extensive information and educational campaigns focused on privacy issues related to Big Data have not only been launched by governments, but also by a broad range of *private sector actors*, including companies, advocacy groups, NGOs, and academic programs. In the US, for instance, the prominent advocacy group Electronic Privacy Information Center (EPIC) provides not only up-to-date resources, but is also engaged in outreach campaigns and user education, among many other activities.[473] Common Sense Education, a leading program of a non-profit organization with a focus on children, media, and technology, provides teachers and schools with extensive research-based tools and curriculums, which include units on privacy protection in the Big Data context.[474] Academic programs such as Fordham's CLIP National Privacy Education Program also include modules and lessons about Big Data applications such as social media.[475]

In addition to educating young users and raising awareness among the public at large, a large number of more targeted efforts have been launched to inform and train specific groups such as business professionals, administrators, or researchers about Big Data privacy issues. In the field of research, for instance, interventions cover a broad spectrum ranging from educational modules as part of a researcher's *IRB training*[476] to the development of tools aimed at improving the assessment and management of privacy risks.[477] As in the other areas mentioned above, some of the most advanced tools under development in this context are software-based and thus go beyond traditional, often text-based educational efforts.[478]

With respect to measures aimed at improving the choice architecture through nudging, a number of initial Big Data scenarios have emerged. In one foundational study, for instance, researchers developed privacy nudges to address the problem that users of social networking sites often do not have a clear idea of who can see their posts – with the consequence that users often post content that can be viewed by unintended audiences, which leads to regret.[479] In order to encourage study participants to reflect on their posts and their audiences, the researchers designed different types of nudges, including a timer nudge «to stop

---

473 See EPIC – Big Data and the Future of Privacy. <https://epic.org/privacy/big-data/>.

474 See Common Sense Media, Scope and Sequence. <https://www.commonsensemedia.org/educators/scope-and-sequence>.

475 See Fordham CLIP Launches National Privacy Education Program, Fordham University, October 16, 2013. <http://law.fordham.edu/31049.htm>.

476 See, e.g., Institutional Review Board Electronic Data Management Policy, SUNY Albany, n.d. <http://www.albany.edu/orrc/assets/Institutional_Review_Board_Data_Management_Policy_v_1_0.pdf>.

477 See, e.g., Privacy Tools for Sharing Research Data, Harvard School of Engineering and Applied Sciences. <http://privacytools.seas.harvard.edu/>.

478 Data Tags, Harvard School of Engineering and Applied Sciences. <http://datatags.org/>.

479 See Wang/Leon/Chen/Komanduri/Norcie/Scott/Acquisti/Cranor/Sadeh (n. 451), pp. 1310–1319

and think, so as to avoid regrettable, ‹spur of the moment› posts,»[480] or a sentiment nudge, which was «designed to help make users more aware of how others might perceive their posts.»[481] In general, the research team found that the nudges induced positive behavioral changes in at least some of the participants.[482]

Insights from behavioral economics are not only applied in field studies, but are also likely to be incorporated into next generation of data protection laws that apply to Big Data scenarios. Specifically, the draft of the European General Data Protection Regulation (GDPR)[483] takes into account cognitive limitations in the context of user consent by introducing behaviorally informed mechanisms such as the obligation for data controllers to use standardized visual icons with traffic-light symbols to better inform users about data collection, processing, and usage practices.[484] As in other areas such as nutrition labels, these traffic light-based visualizations can serve as (here: privacy) nudges.[485]

b. Internet of Things

Human-centered approaches including awareness, education, digital literacy, and improved choice architectures are also elements in policy strategies aimed at dealing with the privacy challenges associated with the Internet of Things, although these concepts are currently less developed in this thematic context when compared to Big Data.

According to a recent FTC Staff Report, for instance, the FTC will increase its involvement in education, developing «new consumer and business education materials» to help users understand «how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings.»[486] Similarly, a factsheet on IoT Privacy, Data Protection, and Information Security published

---

480 Wang/Leon/Chen/Komanduri/Norcie/Scott/Acquisti/Cranor/Sadeh (n. 451), p. 1331.

481 Wang/Leon/Chen/Komanduri/Norcie/Scott/Acquisti/Cranor/Sadeh (n. 451), p. 1331.

482 Wang/Leon/Chen/Komanduri/Norcie/Scott/Acquisti/Cranor/Sadeh (n. 451), p. 1310.

483 European Parliament Legislative Resolution of 12 March 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2014. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>.

484 See Art. 13a and Annex. For a detailed discussion, see Eoin Carolan and Alessandro Spina, Behavioral Sciences and EU Data Protection Law: Challenges and Opportunities, (forthcoming, manuscript on file with author).

485 Calories, We Never Knew You, BloombergView, November 28, 2014. <http://www.bloombergview.com/articles/2014-11-28/calories-we-never-knew-you>.

486 U.S. Federal Trade Commission (FTC) (n. 56), p. viii and p. 8. It is worth noting that some observers expressed surprise that the agency did not put more emphasis on educational approaches; see Adam Thierer, Some Initial Thoughts on the FTC Internet of Things Report, Technology Liberation Front. <http://techliberation.com/2015/01/28/some-initial-thoughts-on-the-ftc-internet-of-things-report/>

by the European Commission mentions and considers user education «throughout all levels of the educational system» as a way to address a series of challenges, ranging from design considerations to difficulty in decision-making processes.[487]

In addition to governmental agencies, *standards-setting bodies* such as GS1 have also emphasized the importance of user education at the intersection of Internet of Things and privacy. Specifically, the Guidelines on EPC for Consumer Products – EPCs are Electronic Product Codes that bridge the world of barcode-based identifiers on the one hand and RFID on the other, and allow products to be identified from distance – cover consumer education in addition to consumer notice, choice, and record use, retention, and security. The Guidelines require that companies «using EPC tags at the consumer level will cooperate in appropriate ways to familiarize consumers with the EPC logo and to help consumers understand the technology and its benefits.»[488]

User education as a supplementing strategy aimed at enhancing Internet of Things privacy – in addition to technical and regulatory approaches – is also discussed in academic contributions. Swiss privacy scholars Rolf H. Weber and Romana Weber in particular call for a comprehensive approach to educate consumers about IoT security and privacy threats. Such efforts would serve two goals, according to the authors: «First, users have to be taught how to safely interact in the IoT. Second, the educated user should also be able to discover a potential for failure and either respond to the threat or contact the responsible organization [...].»[489]

While the discussion about improvements of privacy choice architectures in the Internet of Things environment is still relatively nascent, a number of policy reports and guidelines recognize the *importance of behaviorally informed system designs* that connect physical objects to the Internet. One focus area is privacy-friendly default settings as a way to nudge user behavior. The above-mentioned factsheet on IoT Privacy, Data Protection, and Information Security by the European Commission, for instance, highlights the importance that *privacy by default settings* get implemented in practice and envisions an educational role that data protection officers could play in getting the relevant information to the IT engineers, system designers, and standardization bodies.[490]

A second area where insights from behavioral economics are at least implicitly considered – as in the case of Big Data – relates to the question of *notice and consent*, which is particularly challenging, as there is often no consumer interface in the Internet of Things context. The FTC Staff Report acknowledges

---

487 European Commission, IoT Privacy, Data Protection, Information Security, November 14, 2012. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753>.

488 Guidelines on EPC for Consumer Products (n. 358). For context, see Weber (n. 43), pp. 23–30.

489 Weber/Weber (n. 265), p. 66.

490 European Commission (n. 487).

the resulting practical difficulties of providing choice, but also suggests a number of approaches regarding how to improve notice and choice that are behaviorally informed, including tutorials and set-up wizards, «through which companies could provide clear, prominent, and contextual privacy choices.»[491]

The same rationale also appears in the relevant factsheet by the European Commission, which states that it «needs to be ensured that clear, easily understandable information on the data processing of IoT systems, their objects, functions and purposes, is provided to individuals» and that «[m]echanisms need to be found to make individuals aware of the processing and to provide information on the processor, the purpose of the processing and possibilities to exercise data subject rights, as most IoT applications are expected to operate in the background, invisible to and unrecognised by the individual.»[492]

3. Evaluation

a. Promise

In the age of blended governance regimes, human-centered approaches have gained traction as part of a broader policy discussion about the ways in which the privacy and data protection challenges of our time can be successfully managed. The momentum of techniques like awareness-raising, education, digital literacy and choice architectures as elements of such a human-centered approach comes, broadly speaking, from two main sources: First, human-centered interventions can be seen as a substituting mechanism that compensates for the relative weakness of traditional, especially legal and regulatory, approaches when applied to the next-generation privacy problems. Second, the elements of a human-centered approach outlined in the previous paragraphs can be understood as supporting techniques with the potential to help improve existing mechanisms, such as notice and consent, within the current legal and regulatory framework.

A prominent advocate of human-centered techniques as an *alternative approach* to privacy protection is US privacy scholar Adam Thierer. Building upon experiences with online safety regulation, he argues that user education and empowerment – plus selective enforcement – will be better alternatives than top-down mechanisms, as it is «exceedingly difficult to devise a fixed legal standard for privacy that will be satisfactory for a diverse citizenry (not all of whom value privacy equally),» and as it is «increasingly difficult to enforce that standard even if it can be determined.»[493] From such a perspective, education and awareness efforts that can be deployed at multiple levels and adjusted

491 U.S. Federal Trade Commission (FTC) (n. 56), pp. 39–41.
492 European Commission (n. 487), p. 6.
493 Thierer (n. 402), p. 411.

as needed are less costly and less cumbersome solutions than legal and regulatory regimes.[494]

The benefits of a human-centric set of techniques designed to improve privacy also become visible when looking at it as a *complementary* rather than alternative strategy to law and regulation. As noted, both in the US and in Europe many public and private sector actors have emphasized the role of awareness-raising, user education, and digital literacy as an integral part of a broader effort aimed at protecting consumers in general and tackling current and future digital privacy challenges in particular.[495] Viewed from that angle and at an abstract level, human-centered interventions – for instance in form of educational resources or self-help tools – empower consumers to better navigate the digitally networked environment by successfully identifying and managing privacy risks.[496]

In addition, certain instruments available from the human-centered toolbox have the promise of strengthening the effectiveness of traditional legal methods of privacy and data protection. Techniques to improve existing notice and consent regimes through better user interface design, improved information notices such as standardized traffic-light symbols and other visual icons, or tutorials and set-up wizards are examples in this category.[497] As discussed, both European and US policymakers have promoted – and in some instances may even mandated – such advanced information-based schemes that take into account findings from behavioral science.

With respect to *privacy nudges* specifically, the main promise is to improve privacy by providing additional context – for instance through visual representations or manipulation of the system's default settings – to aid the user's decision about the disclosure of personal information, hereby mitigating the effects of well-known behavioral and cognitive biases on such decisions.[498] The potential benefits of privacy nudges – particularly in form of privacy default settings – have been acknowledged particularly in the European context, while the adoption of such privacy-protecting measures in practice is still in its infancy.

---

494 See Thierer (n. 404), p. 1056.

495 See generally Thierer (n. 402).

496 Thierer (n. 402); see also Pedro Giovanni Leon-Najera, Privacy Notice and Choice in Practice, Dissertation Carnegie Mellon University, 2014. <https://www.andrew.cmu.edu/user/pgl/p_leon_epp_2014.pdf>.

497 See, e.g., Masooda Bashir, Kevin Hoff, Carol Hayes, and Jay Kesan, Knowledge-Based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices, University of Illinois at Urbana-Campaign, n.d. <https://www.cylab.cmu.edu/news_events/events/fopnac/pdfs/bashir.pdf>. See also Najera (n. 495); Irdis Adjerid, Alessandro Acquisti, Goerge Loewenstein, Framing and the Malleability of Privacy Choices. <https://www.cylab.cmu.edu/news_events/events/fopnac/pdfs/adjerid.pdf>.

498 See, e.g., Acquisti (n. 446), p. 74.

b. Limitations

Human-centered approaches to privacy protection have promise, but also significant limitations. With respect to awareness-raising, user education, and digital literacy, a series of limiting factors are noteworthy.

The experience with educational efforts in the field of online child safety – an example frequently cited when advocating for education-based approaches to privacy[499] – demonstrates a *basic conceptual challenge* with information-based strategies: in order to be effective, any educational initiative needs to build upon a deep understanding of the phenomenon it seeks to address.[500] In a complex quicksilver technology environment with rapidly evolving user behavior, the necessary evidence in which educational strategies and messages can be rooted is often not available for some time or becomes outdated quickly. The risk of intervention absent evidence is that resources are misallocated or problems wrongly prioritized – as the case of child online safety demonstrates, where initial efforts overestimated the stranger-danger risk and underestimated peer-based safety concerns such as bullying.[501]

Once research becomes available, its findings are likely to be full of nuance and might be in contrast to basic assumptions by educators.[502] This poses a two-fold challenge that might limit the promise of educational approaches. First, educators need to be willing to take into account research data on an ongoing basis. That requires not only the resources to establish and maintain an effective interface between privacy researchers and educators, but also a commitment to challenge basic assumptions and framings of educational resources as new data becomes available. Second, more data typically means more nuance. For instance, research on youth and privacy demonstrates that not all youth are equally likely to share information and hence not exposed to the same privacy risks. Their online behavior often varies based on age, gender, status, and other variables.[503] Curriculum-based educational efforts, in contrast, will have to

499 See especially Thierer (n. 402), p. 412 («The best way to protect personal privacy in the United States, therefore, is to build on the approach now widely utilized to deal with online child safety concerns …»).

500 See, e.g., Lisa Jones and David Finkelhor, Increasing Youth Safety and Responsible Behavior Online: Putting in Place Programs That Work, (A FOSI Discussion Paper), Family Online Safety Institute, 2011. <http://www.unh.edu/ccrc/pdf/fosi_whitepaper_increasingyouthsafety_d9.pdf>.

501 See John Palfrey, Dena Sacco, and danah Boyd, Enhancing Child Safety & Online Technologies, Final Report of the Internet Safety Technical Task Force, Durham 2008. <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf>; Urs Gasser, Sandra Cortesi and Jan Gerlach, Kinder und Jugendliche im Internet: Risiken und Interventionsmöglichkeiten, Mit einem Beitrag zur digitalen Didaktik von Peter Gasser, Bern 2012.

502 Madden, Mary, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton, Teens, Social Media, and Privacy, Pew Research Center's Internet & American Life Project, 2013. <http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>.

503 See Madden/Lenhart/Cortesi/Gasser/Duggan/Smith/Beaton (n. 502).

work with a certain degree of generalization, which might lead to the unintended consequence that the most-at-risk populations are not adequately addressed.

Awareness-raising and user education also face a *complexity barrier*: the examples of Big Data and the Internet of Things are indicative of the levels of technical, economic, and even basic legal knowledge and understanding that already needs to be in place in order to make issue-specific educational campaigns – for instance on key issues such as new privacy risks associated with re-identification of anonymized data vis-à-vis multiple datasets, or predictive algorithms – successful.[504] The complexity limitation cannot be overcome by simply increasing the amount of educational information: the problem of information overload has been recognized not only in the field of consumer protection generally, but also with respect to privacy specifically and by scholars and policymakers alike.[505]

Another limitation has to do with the ways in which users process and act upon information. A recent literature review by behavioral scientists summarizes this as follows:

> «Insights from the social and behavioral empirical research on privacy [...] suggest that policy approaches that rely exclusively on informing or ‹empowering' the individual are unlikely to provide adequate protection against the risks posed by recent information technologies. Consider transparency and control, two principles conceived as necessary conditions for privacy protection. The research [...] shows that they may provide insufficient protections and even backfire when used apart from other principles of privacy protection.»[506]

Soft paternalistic approaches in general and nudging in particular seek to overcome this last limitation. However, such approaches and techniques are not without challenges either. At the most general level, critics argue that nudging is inherently manipulative, might erode autonomy, and even infantilize users over time.[507] More specific limitations have also been identified with re-

---

504 On the fundamental problem of the role of previous knowledge («Vorwissen») and the limits of information-based approaches see Jean Nicolas Druey, Information als Gegenstand des Rechts, Zürich 1995.

505 See, e.g., Thierer (n. 404), p. 1095; Petra Persson, Attention Manipulation and Information Overload, IFN Working Paper No. 995, 2013. <http://www.ifn.se/wfiles/wp/wp995.pdf>; European Commission, Report on Consumer Policy, January 2012–December 2013, pp. 26–31. <http://ec.europa.eu/consumers/strategy-programme/policy-strategy/documents/consumer_policy_report_2014_en.pdf>.

506 Acquisti/Brandimarte/Loewenstein (n. 151), p. 515; Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, Misplaced Confidences: Privacy and the Control Paradox, Cambridge 2010. <http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf>.

507 See, e.g., Luc Bovens, The Ethics of Nudge, Preference Change: Approaches from Philosophy, Economics and Psychology, Berlin and New York 2008. <http://www.bovens.org/TheEthicsFV.pdf>; Evan Selinger and Kyle Whyte, Is There a Right Way to Nudge? The Practice and Ethics of Choice Architecture, Sociology Compass, Vol. 5, No. 10, pp. 923–935, July 10, 2011;

spect to default rules created by law, which are not always «sticky» and might not prevent individuals from opting out who would be better off within the default.[508] Some of these (general) concerns and limitations have been further explored in the privacy context. Lauren E. Willis, for instance, argues that defaults with opt-out options for users aimed at limiting tracking of users' online behavior are likely to be too slippery, and are not likely to result in well-educated consumers.[509] Nudging proponents have convincingly addressed some of the normative critiques,[510] while other limitations – including practical concerns regarding «slippery» defaults – persist at both the conceptual and implementation level and also with respect to privacy nudges.

4. Outlook

Human-centered approaches to privacy protection are en vogue and – given the attention they receive among experts, activists, policymakers, and other actors – will likely play an increasingly important role in future privacy and data protection regimes on both sides of the Atlantic. Awareness-raising and user education – as information-based strategies – resonate well with the overall trend towards increased transparency and the enhanced role information plays in society. As discussed, such approaches are indeed well suited to address at least some of the challenges outlined in the first part of this report, particularly when designed and implemented as supplementary and complementary rather than substituting approaches.

In the light of the limitations mentioned above, information-based approaches such as awareness-raising and user education seem particularly promising where they are *multi-layered* in the sense of a combination of general education – for instance in the form of digital literacy or 21st century skills – with more specific and ad hoc interventions vis-à-vis particular informational context, services, and associated privacy risks.[511] Moreover, information-based

---

Edward L. Glaeser, Paternalism and Psychology, Regulation, University of Chicago Law Review, Vol. 73, No. 1, pp. 32–38, 2006.

508 Lauren E. Willis, When Nudges Fail: Slippery Defaults, University of Chicago Law Review, Vol. 80, pp. 1155–1229, 2013. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2142989>.

509 Lauren E. Willis, Why Not Privacy by Default?, Berkeley Technology Law Journal, Vol. 29, No. 1, pp. 61–133, 2014. <http://btlj.org/data/articles 2015/vol29/29_1/29-berkeley-tech-l-j-0061–0134.pdf>.

510 See, e.g., Ryan Calo, Code, Nudge, or Notice?, Iowa Law Review, Vol. 99, No. 2, 773–802, 2014, pp. 783–787. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2217013>.

511 In the Internet of Things context, see, e.g. Weber/Weber (n. 265), pp. 65–66. On multi-layered approaches with emphasis on user education and empowerment more generally, see, e.g., Adam Thierer, Why Doesn't Society Just Fall Apart?, Forbes, January 23, 2012. <http://www.forbes.com/sites/adamthierer/2012/01/23/why-doesnt-society-just-fall-apart/>; see also Adam Thierer, The Unintended Consequences of Well-Intentioned Privacy Regulation, Forbes, November 6, 2011. <http://www.forbes.com/sites/adamthierer/2011/11/06/the-unintended-consequences-of-well-intentioned-privacy-regulation/>.

approaches are likely to be most effective where privacy risk disclosures, educational materials, etc. are not only made available to users, but where users have *tools* at hand to interact with such information in a meaningful way, for instance through dashboards, visualization tools, scenario planning, and the like.[512] The effectiveness of awareness-raising and user education, in other words, depends not only on the release of educational resources (broadly defined) that are evidence-based and appropriately tailored to the targeted audience, but also on the building of an infrastructure that supports users to create meaning out of such information.

Elements within the human-centered approach that focus on the social and psychological dimension of user behavior in seeking to confront privacy challenges also show great promise. A growing body of research and field studies demonstrates how insights from behavioral economics can be used to improve notices,[513] better use the power of default settings,[514] and work with privacy nudges where users are chronically making the same mistake in their information behavior, as illustrated above in the context of social networking sites.[515] The discussion suggests that some of these techniques make their way into policy frameworks and already inform the design of legal requirements – for instance in the case of the above-mentioned notice requirements put forth in the draft of the European General Data Protection Regulation – while others are more likely to be incorporated as part of good or best practices by digital service and platform providers.

Looking at human-centric approaches from a broader perspective, such approaches seem most promising where the substantial work that is being done in the educational sphere – including the design and implementation of new curricula and privacy-awareness campaigns, to name just two efforts – is supported by tools that help users to digest such information, and where the work is tinted by a rapidly growing body of behavioral insights to ensure these efforts are maximally effective.

---

512 See, e.g., Dan Auerbach, 4 Simple Changes to Stop Online Tracking, Electronic Frontier Foundation, October 25, 2012. <https://www.eff.org/deeplinks/2012/04/4-simple-changes-protect-your-privacy-online>; Eva Galperin and Jillian C. York, Yes, Online Privacy Really Is Possible, Slate, February 14, 2014. <http://www.slate.com/blogs/future_tense/2014/02/14/threat_modeling_and_finding_the_right_level_of_online_privacy_for_you.html>; Lightbeam for Firefox, Mozilla. <https://www.mozilla.org/en-US/lightbeam/>.

513 See, e.g., Alessandro Acquisti and Jens Grossklags, What Can Behavioral Economics Teach Us About Privacy?, in: Alessandro Acquisti, Stefanos Gritzalis, Sabrina Di Vimercati, Costos Lambrinoudakis (Eds.), Digital Privacy: Theory, Technologies, and Practices, Auerbach Publications, pp. 363–379, Boca Raton 2007. <http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf>; see also Leon-Najera (n. 496).

514 See, e.g., Ausloos/Kindt/Lievens/Valcke/Dumortier (n. 455).

515 Wang/Leon/Chen/Komanduri/Norcie/Scott/Acquisti/Cranor/Sadeh (n. 451); see also Leon-Najera (n. 496).

V. Law-Based Approaches

1. Approach

a. Evolving Privacy Laws

The fourth and final approach to addressing the issues posed by contemporary privacy challenges is law. As discussed earlier, law shapes digital privacy indirectly by guiding the development and evolution of the digital ecosystem, as well as directly by stipulating different norms about the collection, dissemination, and use of personal information in the form of specific privacy laws. In this respect, law can either take a privacy-protective approach or be designed to allow legitimate privacy invasions to happen; examples in the latter category include data retention laws or interception and surveillance laws,[516] and in some instances even tort law.[517] When dealing with privacy challenges in the Internet age, it is helpful to take a step back and reflect on the ways in which privacy laws have responded to new technologies and associated privacy threats in the past.

Privacy-protective legal norms – the focus of the following section – date back to the 19th century, and have emerged and evolved in response to *changes in technology* that increased the collection and use of personal information.[518] For instance, privacy threats resulting from the rise of newspapers, new forms of «yellow journalism» focused on sensational topics, the rise of instant photography, and increased literacy rates not only led to an evolution in the common law of torts,[519] but also to the concept of a «more general right of the individual to be let alone,» as stipulated in the famous 1890 Harvard Law Review Article by Samuel D. Warren and Louis D. Brandeis.[520] The birth of modern information privacy (or data protection) law on both sides of the Atlantic in the 1970s was an «attempt to protect individual privacy rights against the dangers stemming from the collection, storage, manipulation, and dissemination of personal data by the modern organization employing the latest information technology.»[521]

While a series of factors led to the enactment of privacy laws in the US and in Europe, «technology was always a catalyst for public concerns about privacy» and «played a pivotal role in defining [...] issues as public problems and placing them on the policy agenda.»[522] In the US, for instance, the first wave of privacy legisla-

---

516 See, e.g., Paul Bernal, Internet Privacy Rights, Cambridge 2014, pp. 87–111.

517 See Eugene Volokh, Tort Law vs. Privacy, Columbia Law Review, Vol. 113, pp. 879–948, 2014. <http://columbialawreview.org/wp-content/uploads/2014/05/May-2014-7-Article-Volokh.pdf>.

518 See e.g., Solove (n. 171), p. 1-3-1-8.

519 Solove (n. 171), p. 1-3-1-8.

520 Samuel Warren and Louis Brandeis, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, pp. 193–220, 1890.

521 Bennett (n. 171), p. 1.

522 Regan (n. 171), p. 10.

tion, resulting in the Privacy Act of 1974,[523] originated from the introduction of mainframe computers in the 1960s with the goal of articulating privacy values that should govern the use of such technology in organizational settings.[524] Similarly, subsequent pieces of sectoral legislation such as the Children's Online Privacy Protection Act[525] interacted with – and were catalyzed by – technological advancements, in addition to various other factors, including the increased use of personal information in computer databases and the arrival of the Internet.[526]

Technology is also an important factor that has shaped the evolution of privacy laws in Europe. For instance, the first European data protection law – the Hesse Data Protection Act of 1970 – was a direct response to the fear of power shifts across different branches of government as a result of the use of power-enhancing data processing based on large computing systems, as Professor Herbert Burkert points out.[527] In addition, privacy scholars who analyzed the subsequent generations of data protection laws across European countries situated this evolution of data protection laws within the various stages of technological development and corresponding privacy threats with regard to the collection, dissemination, and use of personal information in both the public and private sector.[528] The rationale behind the most recent update to the European data protection framework indicates that the next stages in the evolution of data protection law are also linked to the development and use of new types of digital technologies, including Big Data and the Internet of Things, among others.[529]

b. Response Patterns

When looking at the evolution of privacy laws vis-à-vis technological change, it is important to clarify that legal responses to technological innovation should not be understood as a simple stimulus-response mechanism – despite the rela-

---

523 5 U.S.C. § 552a (1974).

524 See the detailed analysis by Regan (n. 171), Chapter 4: Information Privacy: Recording our Transactions.

525 15 U.S.C. §§ 6501–6506, 1998.

526 See e.g., Solove (n. 171), p. 1-3-1-8.

527 See Herbert Burkert, Privacy – Data Protection. A German/European Perspective, in: Christoph Engel and Kenneth H. Keller (eds.), Governance of Global Networks in the Light of Differing Local Values, pp. 43–70, Baden-Baden 2000.

528 See, e.g., Viktor Mayer-Schönberger, Generational Development of Data Protection in Europe, in: Philip E. Agre and Marc Rotenberg (eds.), Technology and Privacy: The New Landscape, pp. 219–41, Cambridge 1997; see also Omer Tene, Privacy: The New Generations, International Data Privacy Law, Vol. 1, No. 1, pp. 15–27, 2011. <http://www3.nd.edu/~cpence/eewt/Tene2011.pdf>; and Attila Kiss and Gergely László Szoke, Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation, Law, Governance and Technologies Series, Vol. 20, pp. 311–331, 2015.

529 See, e.g., Viviane Reding, The Upcoming Data Protection Reform for the European Union, International Data Privacy Law, Vol. 1, No. 1, pp. 3–5, February 1, 2011; Thibaut Kleiner, The Future of Privacy in the Internet Age, A European Perspective, in: Carine Dartiguepeyrou (ed.), The Futures of Privacy, Cahier de prospective, pp. 83–94, 2014. <http://cvpip.wp.mines-telecom.fr/files/2014/02/14-02-The-futur-of-privacy-cahier-de-prospective.pdf>.

tively close link between technological advancements and the evolution of privacy laws – but rather as the result of complex interactions among different social subsystems and forces at play. Moreover, the legal system is *functionally differentiated* in its responses. On a general level and in the sense of pattern recognition, three analytically distinct (but in practice often interacting and sometimes blurring) types of responses can be identified:[530]

- *Subsumption*, a default response mode in which the legal system and its actors seek to apply old rules to a (new) problem emerging in context of the use of a new technology.
- *Gradual innovation*, where the legal system reacts by «updating» the law vis-à-vis new phenomena either through new precedents or by intervention on the part of the legislature.
- *Paradigm change*, where not only individual existing norms are adjusted, but entire approaches, instruments, or other core elements of a given regime are changed.

Subsumption is the standard response mode when privacy law meets challenges created by the use of new technologies and is at least in part motivated by the desire to preserve the internal consistency of the legal and regulatory system.[531] Courts in the US, for instance, apply privacy torts as they address complaints about improper collection, use, or disclosure of personal data by digital businesses such as Google[532] and Facebook[533] and hereby largely rely on tort conceptions of privacy advanced in the late 19th century.[534] Perhaps not surprisingly, US privacy experts observe that traditional privacy torts have not proven to be a good match for consumer privacy complaints in the digital age.[535] In addition to the courts, policymakers and regulators also typically insist – at least in early phases of change where uncertainty is particularly high for the reasons outlined in the earlier part of this report – on the application of the exiting privacy norms and mechanisms to address digital privacy challenges. Illustrative of this are current discussions both in the EU[536] and in

---

530 The following paragraphs are based on Gasser/Burkert (n. 86), pp. 503–523.

531 See, e.g., U.S. Federal Trade Commission (FTC) (n. 57), p. 16.

532 See, e.g., *Boring v. Google, Inc.*, 598 F. Supp. 2d 695, 699–700 (W.D. Pa. 2009) (dismissing intrusion upon seclusion tort claim for failure to demonstrate that Google's Street View program was highly offensive to a reasonable person of ordinary sensibilities).

533 See, e.g., *Fraley v. Facebook*, Inc., 830 F. Supp. 2d 785 (N.D. Cal. 2011) (discussing applicability of privacy tort of appropriation of name and likeness to Facebook's use of social advertisements).

534 See, e.g., Neil M. Richards, The Limits of Tort Privacy, Journal on Telecommunication and High Technology Law, Vol. 9, pp. 357–384, 2011. <http://www.jthtl.org/content/articles/V9I2/JTHTLv9i2_Richards.PDF>.

535 See, e.g., Neil M. Richards and Daniel J. Solove, Prosser's Privacy Law: A Mixed Legacy, California Law Review, Vol. 98, pp. 1887–1924, December 2010, pp. 1918–1921.

536 Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final—2012/0011(COD), January 25, 2012.

Switzerland,[537] where policymakers reinforce the importance of traditional instruments such as notice and consent, even if their effectiveness in the Big Data age is questionable as best, as prominent scholars have pointed out.[538]

Where the subsumption approach leaves too much room for interpretation to fully satisfy the needs for legal certainty or does not succeed in managing the increased entropy that is created during the phase in which old rules and new problems are confronted, the legal system may react with the *creation of new law*.[539] The enactment of an «Online Eraser» law for minors in the State of California[540] or of the Directive on Privacy and Electronic Communication in the EU[541] are examples of such situations where legislators have responded to shifts in the digital ecosystem and specific problems resulting from it. Going forward and in light of the challenges outlined in the first part of the report, these debates illustrate the broad spectrum of proposals that fall under this category, ranging from relatively modest adjustments of existing norms to more fundamental changes, which might include larger conceptual shifts.[542]

Referring back to the dissatisfactory outcomes of subsumption, an example of a gradual innovation in the US context is the suggestion to adapt tort principles to digital privacy, for instance by introducing a tort for the misuse of personal information by data traders.[543] The recent White House proposal for the Consumer Privacy Bill of Rights Act[544] is a more ambitious example of legal innovation in the digital privacy space, although core elements of the current regulatory approach remain unchanged.[545] In Europe, the proposed General Data Protection Regulation marks the next generation in the evolution of privacy legislation, which involves a more comprehensive overhaul of existing

---

537 The advisory group on the revision of the Swiss Data Protection Act, for instance, proposes to leave the current requirements for consent as laid out by Art. 4 Para 5 DPA unchanged if compatible with the modernization of the Council of Europe's Data Protection Convention 108, see Federal Office of Justice (n. 240), p. 20.

538 See Fred H. Cate and Viktor Mayer-Schönberger, Notice and Consent in a World of Big Data, International Data Privacy Law, Vol. 3, No. 2, pp. 67–73, 2013.

539 See Gasser/Burkert (n. 86), pp. 503–523.

540 Cal. Bus. & Prof. Code §§ 22580 et seq., 2013.

541 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>.

542 See, e.g., Herbert Burkert, Changing Patterns—Supplementary Approaches to Improving Data Protection: A European Perspective, in: Canadian Institute for the Administration of Justice Technology, Law and Privacy, Toronto, pp. 243–258, 2007.

543 See, e.g. Sarah Ludington, Reining in the Data Traders: A Tort for the Misuse of Personal Information, Maryland Law Review, Vol. 66, pp. 140–193, 2006. <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5492&context=faculty_scholarship>.

544 See, e.g., U.S. White House (n. 180).

545 See, e.g., Center for Democracy & Technology, Analysis of the Consumer Privacy Bill of Rights Act, CDT Insights (blog), March 2, 2015. <https://www.cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act>

laws. Specifically, the number of proposed new obligations on data controllers suggest that the proposal «is more relevant than a simple fine-tuning of existing legislation and the focus is clearly on shifting to the issues of ‹what the data controllers shall do›, from the question of ‹what the data subject has the right to›.»[546] It is worth noting that legal innovations can not only be induced by legislators, but also significantly advanced by courts. This is illustrated by several recent cases, such as the influential *Volkszählungsurteil*[547] by the German Federal Constitutional Court with the «right to personal self-determination,» and[548] the controversial *Google Spain*[549] ruling by the European Court of Justice and the resulting «right to be delisted.»[550]

Finally, the debate about the future of digital privacy also indicates a third way in which the legal system can respond to the ecosystem challenges outlined in the first part of this report: by *shifting paradigms* and reengineering privacy protection and legal approaches to privacy more fundamentally. Such far-reaching approaches and proposals, when compared to the previous response mode that introduces new elements to the existing framework, aim to disrupt the way privacy is conceived and enforced in the current legal system. One example of a proposal in this category is the idea of adopting (second generation) regulatory approaches from environmental law to achieve privacy protection goals by incentivizing actors to find the most cost effective way of achieving a set goal rather than requiring the use of specific tools.[551] Another example is the proposal to shift the focus away from concepts that focus on control towards mechanisms that facilitate the flow of various categories of personal information, for instance in the form of data guardians, which would maintain a personal data vault and negotiate and advocate on behalf of their clients about the use of their data vis-à-vis marketers, authorities, etc.[552] The introduction of alternative dispute resolution mechanisms to solve privacy-related conflicts is a third example that indicates a paradigm shift regarding the ways in

546 Kiss/Szoke (n. 528), p. 328.

547 BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

548 See, e.g., Hans Peter Bull, Informationelle Selbstbestimmung – Vision Oder Illusion?, 2., akt. A., Tübingen 2011.

549 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, Court of Justice of the European Union, Grand Chamber, May 13, 2014. <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.

550 See Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on «Google Span and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,» C-131/12, Adopted November 26, 2014. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

551 Dennis Hirsch, Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law, Georgia Law Review, Vol. 41, No. 1, pp. 1–63, 2006. <http://ssrn.com/abstract=1021623>.

552 See, e.g., Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, and Mark Hansen, Self-Surveillance Privacy, Iowa Law Review, Vol. 97, pp. 809–847, 2012.

which law can and should deal with large-scale privacy threats and incidents in the digital age – for instance in the form of private «Cyber Courts» that «would allow for a preliminary settlement of conflicts between freedom of opinion and the protection of personality rights.»[553]

2. *Application*

a. *Big Data*

Confronted with the Big Data phenomenon described in the introduction of this report, courts as well as law- and policymakers have recently started to respond along the patterns identified in the previous section – although these real-world responses often fall between the exact contours of the three response modes, which primarily serve as a heuristic tool.[554] The subsumption approach, as mentioned earlier, is currently the dominant response mode,[555] which plays out particularly in the context of court cases. The US case *Joffe v. Google*, Inc.[556] is illustrative of the subsumption approach, and involved a leading Big Data company. In this case, the court was confronted with the question whether a relatively new technology – local wireless networks (WiFi) – fit under the definition of «radio communication» set forth by the Wiretap Act.[557] The Act had been modernized by the Electronic Privacy Act of 1986 (ECPA)[558] in order to crate new protections for electronic communication in the mode of «gradual innovation,» but the amendments were unable to keep up with the rapid technological advancements.[559] After years of review and multiple appeals, the 9th Circuit Court concluded that data transmitted over a WiFi network is not a «radio communication»

---

553 Karl-Heinz Ladeur, New Institutions for the Protection of Privacy and Personal Dignity in Internet Communication – ‹Information Broker›, ‹Private Cyber Courts' and Network of Contacts, Brazilian Journal of Public Policy, Vol. 3, No. 2, December 2013.

554 See, e.g., Gehan Gunasekara, Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law, International Journal of Law and Information Technology, Vol. 22, No. 2, pp. 141–177, June 1, 2014; Alan R. Toy, Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy, New Zealand Universities Law Review, Vol. 25, No. 5, pp. 938–959, 2013; Rolf H. Weber and Florent Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich 2012.

555 See, e.g., Herbert Burkert, Aktuelle Herausforderungen des Datenschutzrechts im Kontext Nationaler und Internationaler Entwicklungen, in: Astrid Epiney, Tobias Fasnacht, Gaetan Blaser (Hrsg./eds.), Instrumente zur Umsetzung des Rechts auf Informationelle Selbstbestimmung/ Instruments de mise en oeuvre du droit a l'autodétermination informationnelle, pp. 1–18, Zürich 2013; and Thouvenin (n. 70), p. 79.

556 729 F. 3d 1262 (9th Cir. 2013), amended by No. 11–17483, 2013 WL 6905957 (9th Cir. Dec. 27, 2013).

557 Title III of the Omnibus Crime Control and Safe Streets Act of 19682 (Wiretap Act), Pub. L. No. 90–351, tit. III, 82 Stat. 223 (codified as amended at 18 U.S.C. §§ 2510–2521 (2012), 47 U.S.C. § 605 (2006).

558 Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

559 Google was sued as it collected data about such WiFi networks through its Street View cars in order to improve location-based services for mobile phones—but in some instances also collected and stored email passwords and email content.

and is thus not exempt from the Wiretap Act protection. Ultimately, the case demonstrates how «the rapid expansion of the Internet has given courts the difficult task of applying old law to ever changing technologies.»[560]

In Europe, the *Google Spain* case[561] before the European Court of Justice is another example of a subsumptive reaction that leads to gradual innovation when old laws encounter disruptive technologies.[562] The case unfolded between 2010 and 2014. At issue was whether search engines qualified as «data controllers» under the Data Protection Directive 95/46 and, if so, whether search engines are required to remove information about a data subject from their search index. The Directive, however, was enacted in 1995, during a time when «search engines were new phenomena and their current development was not foreseen by the Community legislator.»[563] The Advocate General argued this point, but the Court disagreed, declaring search engines to be data controllers, enabling data subjects to exercise the right to be «delisted» in a new context. This controversial ruling, resulting in hundreds of thousands of requests to delist search results and forcing Google to serve as an adjudicator in privacy conflicts, demonstrates one core problem with the subsumption approach: it typically requires courts to force new facts under existing definitions that the legislator did not have in mind when drafting the relevant norms, potentially leading to normative overreach.[564]

Subsumption, gradual innovation, and paradigm changes are not limited to the courts; policymakers and regulators also seem to respond to emerging technologies in these modes as well, particularly subsumption and gradual innovation. The US FTC, for example, does not have any special or express authority to regulate information privacy laws on the Internet. In 1997, at the behest of Congress, the FTC became the de facto regulatory of Internet privacy in the US by subsuming website privacy policies under its «unfair and deceptive trade practices» authority.[565] Responding to assertion that data protection principles

---

560 Federal Statutes—Wiretap Act—Ninth Circuit Holds that Intercepting Unencrypted Wi-Fi Broadcasts Violates the Wiretap Act, Harvard Law Review, Vol. 127, April 2014, p. 1855.

561 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, Court of Justice of the European Union, Grand Chamber, May 13, 2014. <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.

562 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, Court of Justice of the European Union, Grand Chamber, May 13, 2014. <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.

563 Advocate General's Opinion in Case C-131/12 Google Spain SL, Google, Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzales, Press Release No. 77/13, Luxemborg, June 25, 2013 <http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf>.

564 See, e.g. Eleni Frantziou, Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos, Human Rights Law Review, Vol. 14, No. 4, pp. 761–77, December 1, 2014.

565 Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, Columbia Law Review, Vol. 114, pp. 583–676, 2014. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913>.

should be reviewed in light of Big Data, the EU Article 29 Data Protection Working Party released an opinion in September 2014 affirming that the Data Protection Directive framework is «applicable to the processing of personal data in Big Data operations.»[566] Meanwhile, other policymakers' reactions fit more squarely into the gradual innovation mode. For example, the White House suggested that the aging US Electronic Communications Privacy Act should be amended through legislation to provide more meaningful protections in the age of Big Data.[567] Similarly, the debate in Switzerland about the reform of the Swiss Data Protection Act and the suggestion to more broadly encompass Privacy by Design rather than focusing only on data access controls is an example of gradual evolution.[568] Finally, new approaches in the mode of major paradigm changes, such as introducing legislation modeled after approaches to environmental protection or the allocation of property-rights in data, are more popular with scholars but do not seem to have caught on with policymakers and legislators.[569]

b. Internet of Things

As described in the first part of the report, the Internet of Things is a rapidly evolving, but relatively new technology, and the exact contours of the privacy implications – as well as the appropriate legal responses – have still to be explored in detail.[570] As a result of the newness of the IoT, direct litigation, judicial interpretation, or even legislative action have not yet been observed. Rather, the primary forum through which law has shaped the IoT space is regulatory interpretation promulgated by the relevant regulatory authorities. In addition to the regulatory interpretation occurring in the field, researchers are also exploring the applicability of existing legal structures to the Internet of Things and play a significant role in shaping potential avenues for paradigm changes. While still in the early stages, one can already observe across these debates –

---

566 Article 29 Data Protection Working Party (n. 57), p. 2.

567 U.S. White House (n. 56), p. 49.

568 Schweizerischer Bundesrat (n. 231), p. 350.

569 See, e.g., See Alexandre Flückiger, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, Aktuelle Juristische Praxis, pp. 837–864, 2013, p. 858 et seq., arguing for the interpretation of the right to informational self-determination as a sui generis property right of one's data; see further Thomas Hoeren, Sieben Beobachtungen und eine Katastrophe. sic!, pp. 212–217, 2014, p. 216, voicing concern about the fact that the discussion of property rights for data is missing from the Swiss process of intellectual property law reform.

570 See U.S. Federal Trade Commission (FTC) (n. 56), p. 2 («[T]hese connected devices … will collect, transmit, store, and potentially share vas amounts of consumer data, some of it highly personal.»); Article 29 Data Protection Working Party (n. 65), p. 15 («In the context of the IoT, the processing of an individual's personal data is likely to affect significantly his/her fundamental rights to privacy and to the protection of personal data in situations where, without IoT devices, data could not have been interconnected or only with great difficulty.»).

at least in broad strokes – that subsumption, gradual innovation, and paradigm shifts are response modes under consideration.

Subsumption is clearly the *dominant legal approach*. Both the US and Europe regulators have sought to situate the regulation of Internet of Things devices and services squarely within existing legal frameworks and established regulatory authorities. For example, following a series of workshop meetings with IoT stakeholders, the FTC concluded that the existing notice and choice regulatory model, where companies are required to give consumers a choice regarding the use of personal information following adequate disclosures, «remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT.»[571] Similarly, in the EU, the Article 29 Data Protection Working Party concluded that the existing data protection legal frameworks applied to the IoT and all members of the collection and processing chain.[572] For instance, by applying the existing notice and consent regime of Article 5(3) of Directive 2002/58/EC, the Working Party concludes that «stakeholders in the IoT must ensure that the person concerned has effectively consented to such storage and/or access, after obtaining clear and comprehensive information from the controller about, *inter alia*, the purposes of the processing.»[573] As illustrated by these two examples, subsumption has thus far played a significant role as a response mode to the privacy challenges associated with the Internet of Things, particularly as regulators seek to legitimate their authority over this emergent domain.

Although significantly less prominent than subsumption, examples of regulators in the US opening up to gradual innovation of regulatory authority has occurred in the Internet of Things space. For example, the FTC Staff Report acknowledged the limitations of the notice and choice approach «when there is no consumer interface, and recognize[d] that there is no one-size-fits-all approach.»[574] In response to this challenge, the Staff Report indicated a willingness to experiment with a use-based model that would eliminate the notice requirement in circumstances where a use is «consistent with the context of the interaction – in other words, it is an expected use.»[575] In contrast, the Article 29 Working Party was less open to considering gradual innovation, even when stakeholders were concerned that the existing data minimization requirements «can limit potential opportunities of the IoT, hence be a barrier for innovation, based on the idea that potential benefits from data processing would come from

571 U.S. Federal Trade Commission (FTC) (n. 56), p. 39.

572 Article 29 Data Protection Working Party (n. 65), p. 10 («The relevant legal framework to assess privacy and data protection issues raised by the IoT in the EU is composed of Directive 95/46/EC as well as specific provisions of Directive 2002/58/EC as amended by Directive 2009/136/EC.»).

573 Article 29 Data Protection Working Party (n. 65), p. 14.

574 U.S. Federal Trade Commission (FTC) (n. 56), p. 41.

575 U.S. Federal Trade Commission (FTC) (n. 56), p. 43.

exploratory analysis aiming to find non-obvious correlations and trends.»[576] Instead, the Article 29 Working Party committed to the subsumption approach, concluding that «data minimization principles plays an essential role in the protection of data protection rights granted by EU laws as individuals, so that it should be respected as such.»[577]

A series of policy reports in both the US and EU demonstrate to varying degrees to which regulators envision either subsumption and gradual innovation as a response mode vis-à-vis the privacy challenges of IoT. So far, however, more radical paradigm changes are currently only examined in legal scholarship, where there is consideration of more fundamental reforms to the legal system and its approach to the IoT. For example, Swiss legal scholar Professor Rolf H. Weber has discussed the shortcomings of existing national and regional legal regimes when it comes to the IoT, particularly given the prevalence of cross-border data flows.[578] Instead of local governance, he argues that «the introduction of an international legislator may be required to satisfy the interests of civil society globally.»[579] He goes on to suggest that a dedicated expert governance forum «would permit coordination on a global level and create a new authority responsible and accountable for IoT governance,»[580] but also acknowledges that such a shift may be too dramatic to be accomplished in a reasonable timeframe.[581]

3. Evaluation

a. Promise

Law-based approaches to address the digital privacy crisis are intensively discussed across the Atlantic, with *major privacy reform projects* or at least reform debates underway in the US, Europe, and Switzerland. But not only have lawmakers and regulators started responding to the deeper-layered shifts in the digital ecosystem: *courts* too are dealing with increasingly prominent cases – consider, for instance, the *Google Spain* case at the European Court of Justice[582] or the *Google Streetview* ruling by the Swiss Federal Supreme Court[583] – with the new or at least accelerated issues regarding the collection, dissemination, and use of personal information in the digitally connected environment. As discussed, the legal responses follow a pattern known from the past, which

576 Article 29 Data Protection Working Party (n. 65), p. 16.
577 Article 29 Data Protection Working Party (n. 65), p. 16.
578 See Weber/Weber (n. 265), p. 27.
579 Weber/Weber (n. 265), p. 29.
580 Weber/Weber (n. 265), p. 29; Weber (n. 43), p. 28.
581 See Weber/Weber (n. 265), p. 30.
582 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, Court of Justice of the European Union, Grand Chamber, May 13, 2014. <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.
583 BGE 138 II 346 = Entscheid 1C_230/2011, May 31, 2012.

includes a mix of the application of old rules to new phenomenon, adjusting and updating existing rules, and – more slowly – considering deeper-layered reform and novel approaches to the problem. In this respect, the legal system and its actors can build upon a rich body of experience, including tested methods, on how to deal with technological change.

The benefits of law-based approaches to the digital privacy crisis are manifold and can be derived from the general advantages that legal solutions to societal problems offer. With respect to digital privacy, at least two aspects seem particularly noteworthy. First, legal solutions to the digital privacy challenges of our time come with more *legitimacy* than some of the other types of approaches discussed in this report, as the state «has democratic legitimization, the procedural setup, and institutional enforcement to make regulations [...].»[584] Second, each response mode outlined above follows a particular procedure, which not only increases outcome legitimacy, but also provides opportunities to *synchronize changing social and legal norms*,[585] and more broadly engage in structured normative conversations as an important mechanism for society to cope with hard problems, value trade-offs, etc. under conditions of complexity and uncertainty, as outlined in the first part of the report.

As current privacy debates illustrate, legislators and regulators have a number of macro-regulatory *modes and strategies* available when pursuing particular policy objectives and addressing legal and regulatory issues in complex systems such as innovative high-tech environments.[586] As noted in an earlier section, available modes of regulation include direct intervention by the government, processes of co-regulation, and mechanisms of industry self-regulation.[587] Similarly, the legal and regulatory «toolbox» includes a range of (general) strategies such as command-and-control, incentive-based regulation, and market-harnessing controls, among others, that can be applied to the digital privacy problem in nuanced ways,[588] taking into account the conditions of uncertainty, where outcomes of interventions are often unpredictable.[589] One re-

---

584 Viktor Mayer-Schönberger, The Shape of Governance: Analyzing the World of Internet Regulation, Virginia Journal of International Law, Vol. 43, pp. 605–673, 2002, p. 612.

585 See, e.g., Weber (n. 14), p. 35 and p. 42; and Rolf H. Weber, Proliferation of «Internet Governance,» in: Jonathan Zittrain, Robert Faris, Rebekah Heacock Jones (eds.), Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse, Berkman Center Research Publication No. 2014–17, pp. 138–144, December 15, 2014. <http://papers.ssrn.com/abstract=2538813>.

586 See, e.g., Robert Baldwin and Martin E. Cave. Understanding Regulation: Theory, Strategy, and Practice, Oxford, 1999.

587 See, e.g. Von Lewinski, (n. 9), pp. 64–86.

588 See, e.g. Rolf H. Weber, How Does Privacy Change in the Age of the Internet?, in: Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval (eds.), Internet and Surveillance: The Challenges of Web 2.0 and Social Media, pp. 273–293, New York 2013.

589 See, e.g., Andrew Murray, Conceptualizing the Post-Regulatory (Cyber)state, in: Roger Brownsword and Karen Yeung (eds.), Regulating Technology: Legal Futures, Regulatory Frames and Technological Fixes, Oxford, pp. 287–315, 2008, p. 291.

cent study with focus on digital privacy, for instance, identifies and describes five different strategies that future legislation and regulation could encompass: right-to-know legislation that keeps users informed; prohibition legislation that limits certain collection and distribution practices of personal information; IT-security legislation aimed at establishing security standards; utilization regulation that restricts certain uses of data that has been collected; and task-force legislation supporting the technical community's efforts to address privacy challenges.[590]

Finally, the promise of law-based approaches to the digital privacy crisis goes *beyond* traditional privacy laws. For instance, horizontally applicable laws such as competition or contract law can play a key role when addressing privacy challenges in the Internet age. Consider, for instance, how a reinterpretation of traditional contract doctrine might level the asymmetric power relationship between users and large online companies, which – at least in the US – heavily rely on privacy policies that are currently not considered contracts,[591] or how different legal requirements vis-à-vis click-through terms of services might change the current landscape.[592] While the specific costs and benefits of such strategies remain to be analyzed in detail, these examples at least indicate how other areas of law might be activated more strategically and systematically when addressing the digital privacy crisis, whether in the form of direct or indirect modes of intervention and regulation.

b. Limitations

Law-based approaches aimed at addressing the digital privacy crisis are confronted with a series of challenges and resulting limitations, which become visible from a number of complementary analytical perspectives. From a privacy-specific perspective, for instance, leading scholars have demonstrated that the dominant *rights-based approach* in the consumer privacy space is generally «not effective in guaranteeing information governance» and has resulted in a «chasm between broad and deep information privacy rights on the books, and the disturbingly limited enforcement of these rights in practice and through courts.»[593] A more general set of limitations becomes visible from a cyberlaw perspective, which highlights a series of more *fundamental limiting factors* in

---

590 Weber (n. 588), p. 283.

591 See, e.g., Daniel J. Solove and Paul M. Schwartz, Privacy Law Fundamentals 2013, Portsmout, 2013, p. 134.

592 See, e.g, Christina L. Kunz, John E. Ottaviani, Elaine D. Ziff, Juliet M. Moringiello, Kathleen M. Porter and Jennifer C. Debrow, Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements, The Business Lawyer, Vol. 59, No. 1, pp. 279–312, November 2003. See also Bruno Baeriswyl, «Soziale Netzwerke» – Taktgeber für die Reform des Datenschutzrechts, in: Rolf H. Weber and Florent Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, pp. 84–103, Zürich 2013.

593 Viktor Mayer-Schönberger, Beyond Privacy, Beyond Rights – Toward a Systems Theory of Information Governance, California Law Review, Vol. 98, No. 6, pp. 1853–1885, December

connection with the application of law in the digitally networked environment.[594] Issues regarding the use of law-based approaches in the context of the Internet, for instance, range from a lack of acceptance of legal norms by the market participants where the law does not sufficiently take into account practical needs; the lack of lawmaker's technical knowledge; the path dependency of laws when enacted; as well as broader concerns about enforceability in the globalized context.[595]

A governance perspective indicates that the *regulatory state* of the ecosystem – as outlined in the earlier parts of this report – in which law-based approaches have to operate when addressing the digital privacy crisis is characterized by a series of attributes that are also present in other areas of modern governance:[596] a great variety of partly overlapping or otherwise interacting privacy norms has emerged, enacted by a plurality of state actors ranging from national government agencies to supranational institutions with formal rule making capacity, leading to problems of fragmentation.[597] Further, as indicated earlier, a variety of control mechanisms are simultaneously at play, ranging from traditional, command-and-control-based mechanisms to alternative modes of control, such as market regulation, the shaping of social norms, and design requirements. Related, the ecosystem in which the digital privacy unfolds is characterized by a variety of governors. While traditional state regulatory bodies – such as government agencies or courts – continue to play an important role in the context of digital privacy, important control functions that affect digital privacy have also been attributed to alternative «rule makers,» including large companies and standard-setting bodies. Finally, law-based approaches are confronted with an increasing variety of controlees – not only including a large number of businesses that make use of digital technologies and collect and use personal information, but also users who are now active creators and processors of information,[598] in addition to governmental institutions.

Taken together, these perspectives confirm the high complexity and unclear causalities that characterize the ecosystem in the digital privacy context, and in-

---

2010, p. 1875. <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1058&context=californialawreview>.

594 See, e.g., Weber (n. 176), pp. 64–76.

595 See, e.g. Schönberger (n. 584), p. 614; Weber (n. 176), pp. 69–70.

596 See generally Colin Scott, Regulation in the Age of Governance: The Rise of the Post Regulatory State, in: Jacint Jordana and David Levi-Faur (eds.), The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance, pp. 145–174, Cheltenham 2004. On the post-regulatory state of cyberspace see Murray (n. 589), pp. 287–315.

597 See, e.g., Christopher Kuner, Transborder Data Flow Regulation and Data Privacy Law, Oxford 2013.

598 For an example of the privacy implications of this shift, see, e.g. Flora Garcia, Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators, Fordham Intellectual Property, Media and Entertainment Law Journal, Vol. 15, No. 4, pp. 1204–1243, 2005. <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1335&context=iplj>.

dicate conceptual, implementation, and assessment limitations when deploying law-based approaches and activating the above-mentioned response modes. *Conceptual challenges* that might limit what law-based approaches can do include, for instance, the problem of justification of interventions, the problem of trade-offs, and conflicting governance goals.[599] *Implementation issues* range from the limited ability to define the most appropriate timing for intervention (given the dynamics at play, as seen in the first part of this report), to the problem of appropriate selection of regulatory strategies and modes under conditions of uncertainty, and the management of cross-jurisdictional issues.[600] Finally, law's effectiveness might be limited by the current lack of methods and metrics to measure success and evaluate the undesired or unintended consequences of law-based privacy interventions – such as stifling innovation.[601]

4. *Outlook*

Law-based approaches have played, as discussed in the second part of the report, and will continue to play an important role in shaping and directing the future of digital privacy, as both the larger trend towards the «legal enclosure» of cyberspace (*Verrechtlichung* in German) and the analysis of response patterns in this section indicate.[602] The significance of law's contribution and its effectiveness in helping to solve – or at least manage – digital privacy challenges at the intersection of technology, markets, and norms depends on many variables, as suggested in the preceding paragraphs. Three variables are worth highlighting again.

First, a key factor of – and arguably even a prerequisite for – *future success* is the ability to reach at least partial and temporary societal consensus on privacy norms in their respective contexts,[603] and the ability to structure the legal system's interface[604] in a way that allows such pre-legal norms, when sufficiently stable, to enter the legal system and interact with each other.[605] Second,

---

599 See for the cloud context Gasser (n. 85). See also Ian Brown and Christopher T. Marsden, Regulating Code: Good Governance and Better Regulation in the Information Age, Cambridge 2013.

600 See, e.g., Dan Jerker Svantesson, Extraterritoriality in Data Privacy Law, Copenhagen 2013.

601 See, e.g., Adam D. Thierer, A Framework for Benefit-Cost Analysis in Digital Privacy Debates, George Mason Law Review, Vol. 20, No. 4, pp. 1055–1105, 2013. <http://papers.ssrn.com/abstract=2309995>.

602 Weber (n. 14), p. 17.

603 Nissenbaum (n. 186, 2009).

604 For a description of such a mechanism, see Urs Gasser, Kausalität und Zurechnung von Information als Rechtsproblem, München 2002.

605 See also Weber (n. 14), pp. 41–44, and Eva Maria Belser, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Astrid Epiney, Tobias Fasnacht, Gaetan Blaser (Hrsg./eds.), Instrumente zur Umsetzung des Rechts auf Informationelle Selbstbestimmung/Instruments de mise en eeuvre du droit a l'autodétermination informationnelle, pp. 19–45, Zürich 2013.

the legitimacy and performance of law-based approaches will heavily depend on the question of whether legal interventions aimed at protecting privacy can be successfully synchronized with evolving technologies, which does not necessarily require speeding up the response cycles mentioned before, but more importantly requires the incorporation of mechanisms of learning within any privacy regime.[606] A third important variable is whether next generation models and designs for legal interoperability can be developed and deployed in ways that not only enable heterogeneous privacy norms and actors to work together, but also coordinate the plurality of regulatory modes, strategies, and tools available and at play.[607]

The variables highlighted here confirm again – from both a legitimacy and performance perspective – the importance of considering, designing, applying, and evaluating law-based approaches aimed at securing the future of digital privacy in the context of the various technological, economic, and social forces at play. Moreover, these remarks also confirm that the role of law in addressing the privacy challenges associated with Big Data and the Internet of Things has to be seen far beyond privacy law. Harnessing law's full potential here not only requires the activation and involvement of other areas of law, but also moving it beyond its traditional functions of a constraint, enabler, or leveler. Specifically, one of the law's main contributions in addressing privacy challenges in the digital age might not only be the protection of the vulnerable, but also the important task of *coordinating* among the different modes of governance and associated actors.[608] Consumer protection law, for instance, can coordinate and promote educational models, and competition law ensures that competitive business models can flourish, etc.

VI. Conclusions

As discussed earlier in the report, the digital privacy crisis has to be understood in the context of larger shifts in the digital ecosystem. As a result of the complexity of the ecosystem and in light of the conditions of uncertainty, a broad range of approaches needs to be considered when addressing the digital privacy challenges. Mirroring the analysis of key forces at play, the previous section highlighted four types of available approaches as part of a proposed *blended governance* regime, and explored their respective promise and limitations

606 See also GASSER (n. 85), p. 28.

607 See generally PALFREY/GASSER (n. 10); and ROLF H. WEBER, Legal Interoperability as a Tool for Combatting Fragmentation, Centre for International Governance Innovation and the Royal Institute of International Affairs, 2014. <https://www.cigionline.org/sites/default/files/gcig_paper_no 4.pdf>.

608 See, e.g, RICHARD H. MCADAMS, The Expressive Powers of Law: Theories and Limits, Cambridge and London 2015.

when directed at shaping the future of digital privacy: technology-based, market-based, human centered, and law-based.

Technological approaches to the digital privacy crisis encompass a variety of different mechanisms including PETs and Privacy by Design, which can also be applied to both Big Data and IoT challenges. Emphasizing early intervention and prevention rather than ex post and ad hoc measures, technology-based approaches generally – and Privacy by Design specifically – are promising because they operate on the system level and do not rely on individuals. However, significant limits still exist to the effectiveness of such approaches, including incentive and implementation problems. The future success will largely depend on the interplay between technological and legal and regulatory approaches, which indicates the importance of good interface design between these instruments.

Market-based mechanisms – including *reputational effects, business model competition*, and voluntary self-regulation – are another approach available to address digital privacy challenges. Given the dominance and failure of self-regulatory schemes in certain parts of the consumer privacy landscape, particularly in the US, market mechanisms have been met with increasing skepticism in recent years. Studies have shown reputation and consumer demand to be largely ineffective in influencing companies' privacy practices, largely due to a number of biases and information asymmetries. While emerging business models that include privacy-respecting services hold some promise, the outcome of this is uncertain. Despite these many limitations, however, market-based approaches should not be discounted as part of a mixed governance approach as proposed in this report.

Human centered and behavioral approaches may also be used to manage privacy challenges that emerge in the contemporary digital ecosystem. The report discussed strategies ranging from *awareness raising* or education to *«soft paternalism»* (e.g. improving the choice architecture). Human-centered approaches show promise in that they can compensate for certain weaknesses in traditional regulatory approaches, as well as help to improve the effectiveness of existing mechanisms in the legal and regulatory framework. Such approaches can thus be complementary to other privacy-improving techniques. The complexity of the overall ecosystem and its constant evolution as well as the changing conceptions of privacy create significant challenges for the application of human-centered approaches.

Finally, law-based approaches play a key role when addressing contemporary digital privacy challenges. Law-based approaches have the potential to influence digital privacy both indirectly, by shaping the digital ecosystem, and directly, by stipulating privacy specific norms and regulations. Legal approaches are promising for a number of reasons, including their ability to *increase the legitimacy* of outcomes and *stabilize* evolving privacy norms. The broad legal and regulatory «toolkit» available also makes law a relatively flexible approach

in light of the complexity of the digital ecosystem. Along with these promises, however, come a number of limitations, including the path dependency of laws, lawmakers' lack of technical knowledge, and concerns about fragmentation, jurisdictional issues, and enforceability.

D. Designing for the Future

I. Towards Blended Governance

This report has argued that the current digital privacy crisis needs to be understood as part of deeper tectonic shifts in the ways in which information is created, shared, accessed, and used in the globalized digital world. These shifts, in turn, are the product of a multi-directional, multi-level, and highly dynamic interplay among technical, economic, human, and legal forces. As a consequence of the resulting complexity, which was developed within the core argument of this report, the solution space of approaches to multi-faceted digital privacy challenges needs to consider models, strategies, and instruments that span technology, markets, human behavior, and the law and combine these various approaches within a blended governance framework for the future of digital privacy. Such an approach will result in what Professor Viktor Mayer-Schönberger describes as «a *system* of information privacy protection that is much larger, more complex and varied, and likely more effective than individual information privacy rights»[609] that incorporates feedback loops and other mechanisms for learning and future improvement.[610]

While this report has provided an overview of some of the core elements of such a blended governance framework and examined the (potential) contributions of each approach,[611] the question remains open how the different elements can *work together* and be *coordinated* – which is in many situations a prerequisite of their effectiveness, as discussed in the previous section. Insights from interoperability theory and research on multi-stakeholder processes offer at least a starting point for an answer to this open question, which deserves more research, and – perhaps most importantly – experimentation and learning in practice. An emerging *normative theory of interoperability*, for instance, provides guidance on how systems – including governance frameworks – can be designed in situations where various components of the complex system need to

609 Mayer-Schönberger (n. 593), p. 1883.

610 See, e.g. Sandra D. Mitchell, Unsimple Truths: Science, Complexity, and Policy, Reprint edition, Chicago 2012, p. 103.

611 See also Lea Aeschlimann, Rehana Harasgama, Flavius Kehr, Christoph Lutz, Veselina Milanova, Severina Müller, Pepe Strathoff, Aurelia Tamò, Re-Setting the Stage for Privacy: A Multi-Layered Privacy Interaction Framework and Its Application, in: Sandra Brändli, Rehana Harasgama, Roman Schister, Aurelia Tamò (Hrsg.), Symbiose oder Parasitismus, Bern 2014.

work together across the technological, data, human, and institutional layers.[612] Interoperability theory also offers a conceptual approach to overcome the binary choice between harmonization and fragmentation of privacy norms and mechanisms.[613]

Extensive research into governance models indicates how different actors might work in concert towards a blended governance framework from a process perspective. It demonstrates that *multistakholder governance processes* are often most effective in the spaces where traditional approaches, including government-led approaches, are insufficient or impossible.[614] Although «multistakeholder governance» is a difficult to define term,[615] it generally refers to shared governance structures operating on the fringes of traditional governance institutions that include the participation of all parties necessary for successfully and legitimately developing and deploying a solution.[616] Given the breadth of solution space that this report has described, it is worth considering whether a distributed, multistakeholder governance architecture might be helpful when developing an equally distributed set of tools – not as a replacement for privacy legislation, but as a possible coordination mechanism when designing and ultimately implementing a blended governance framework for the future of digital privacy.

In parallel, *academia* can assist in the creation of a robust blended governance framework by making contributions at three levels.[617] First, academic research plays a key role in establishing an evidence-base for future policy decisions concerning digital privacy across the private and public sector, including risk analysis. For instance, researchers may engage in collecting data in order to understand the magnitude of a given privacy challenge – for example in the context of the right to be forgotten.[618] Or research plays a vital role in better understanding user behavior, as the work on behavioral economics and the work on youth, digital media, and privacy featured earlier in this report illustrates.

---

612 See PALFREY and GASSER (n. 10), Chapter 1: The Technology and Data Layers, and Chapter 2: The Human and Institutional Layers.

613 See, e.g., WEBER (n. 607), p. 5.

614 See generally URS GASSER, RYAN BUDISH and SARAH MYERS WEST, Multistakeholder as Governance Groups: Observations From Case Studies, Berkman Center for Internet & Society Research Publication 2015–1, January 15, 2015. <http://ssrn.com/abstract=2549270>.

615 URS GASSER/BUDISH/MYERS WEST (n. 614), p. 8.

616 URS GASSER/BUDISH/MYERS WEST (n. 614), pp. 17–19.

617 On the role of academia in Internet governance debates see, e.g., URS GASSER, Toward an Enhanced Role of Academia in the Debates About the Future of Internet Governance – From Vision to Practice, in: Jonathan Zittrain, Robert Faris, Rebekah Heacock Jones (eds.), Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse, Berkman Center Research Publication No. 2014–17, pp. 134–137, December 15, 2014. <http://papers.ssrn.com/abstract=2538813>.

618 For instance, the Chilling Effects project at the Berkman Center for Internet & Society is documenting takedown notices to study the effects of certain aspects of copyright legislation in the US. See <https://www.chillingeffects.org/>.

Second, academia can serve as a neutral platform to facilitate difficult normative conversations among the various stakeholders, for instance when debating value trade-offs and other sensitive issues. Third, academic research in various disciplines has made and will make important contributions to enhancing and expanding the different elements of the «toolbox,» ranging from the development of next-generation privacy protecting technologies, engagement in robust scenario analysis, to studies and recommendations regarding governance mechanisms for a complex und uncertain, digitally connected and globalized world.

Finally, *all parts of society* – including the providers of digital technologies as well as end users – should engage in an open and ongoing dialog across boundaries and demographics about the future of digital privacy, changing technology, and evolving norms. Perhaps most importantly, such a societal debate leads not only to increased levels of privacy awareness, but also stimulates conversations about and potentially lays the foundation for a much-needed *new privacy ethic* for the digital age.[619] A new ethic would include elements of self-constraint vis-à-vis almost limitless technological possibility related to the collection, dissemination, and use of information, and might ultimately even translate into the development of a new generation of «Fair Information Technologies.»[620]

II. Summary of Observations

Taking a phenomenon-oriented and interdisciplinary approach, this report has engaged in an analysis of a series of real-world examples and developments from the US, Europe, and Switzerland that unfold at the intersection of technology, markets, social norms, and law. The goal of the report has been to explore the characteristics of today's digital privacy crisis, identify its sources, understand the drivers behind it, and map possible solutions and approaches to the future of privacy for consumers in the digital age. In terms of problem framing and analysis, the discussion has revealed the following key points:

- *Big Data* and the *Internet of Things* mark the current frontier of digital technology in a complex networked information environment. An analysis of these phenomena and related trends from a privacy angle indicate that privacy and privacy-related challenges have to be contextualized as part of *lar-*

619 See, e.g., Luciano Floridi, The Fourth Revolution: How the Infosphere Is Reshaping Human Reality, Oxford 2014, pp. 217–220. See also Kirsten Martin, Understanding Privacy Online: Development of a Social Contract Approach to Privacy, Journal of Business Ethics, February 2015. <http://link.springer.com/article/10.1007%2Fs10551-015-2565-9>.

620 See Thorsten Busch, Fair Information Technologies, The Corporate Responsibility of Online Social Networks as Public Regulators, Dissertation University of St. Gallen, 2013. <http://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4139/$FILE/dis4139.pdf>.

ger tectonic shifts with regard to the ways in which information is created, distributed, accessed and used in the digital age.

- The discussion of these two phenomena, which serve as guiding cases used in this report to illustrate both problems and solutions – illustrates the enormous societal benefits of cutting-edge and evolving digital technology and its adaption and use, but also a series of *fundamental challenges* for traditional privacy protection mechanisms, as well as new or at least amplified privacy concerns and cumulative effects, with consequences for individual autonomy and society at large.
- A closer look at the underlying dynamics of the use cases and the surrounding environment from which the diverse set of privacy challenges emerge, reveals a multi-dimensional *interplay among technical, economic and behavioral factors*. Perhaps counter-intuitively, the legal system has also contributed to the current state of affairs, and is partly responsible for the digital privacy crisis.
- Taken together, an analysis of the use cases Big Data and the Internet of Things, and the discussion of the relevant ecosystem in which these phenomena evolve, paint a *complex system* characterized by incomplete and asymmetric information, paradoxical user behavior, and high speed of change – features that have implications both for the analysis of the digital privacy problem as well as possible approaches to address it.

Against the backdrop of the proposed ecosystem perspective, and in the light of the findings related to the key forces at play, the report argues that a *blended governance approach* is needed to manage the current digital privacy crisis practically and from a policy perspective. The core components of the envisioned blended governance framework include four interacting, but analytically distinct elements that come with promises as well as limitations. Specifically:

- *Technology-based approaches* such as privacy enhancing technologies, Privacy by Design, but also recent advancement like differential privacy, are based on the use of technology and related methods to enhance rather than invade digital privacy. The discussion of the selected techniques and their application to Big Data and the Internet of Things demonstrate significant promise, as these approaches consider privacy before – not after – the development and use of technology and are also promoted by policymakers on both sides of the Atlantic.
- *Market forces* have been instrumental in making and shaping of today's digital privacy crisis. That said, a discussion of mechanisms including reputational effects, evolving business models, and other market-based approaches suggest at least modest ways in which market forces may actually lead to more privacy-respecting services, especially when seen as part of a larger governance effort and in the spirit of overcoming the traditional, but unhelpful and outdated dichotomy between market-based solutions and government regulation.

- Privacy experts across the world stress the importance of equipping users with the necessary *knowledge, tools, and skills* to understand and manage the multi-faceted digital privacy challenges of our time. Approaches discussed in the report include awareness raising, education, and digital literacy programs. Further, other important strategies that fall in the category of a human-centric approach – such as «privacy nudges» – have been discussed in the light of Big Data and the Internet of Things, with a guardedly optimistic assessment of their contribution when ensuring the future of digital privacy.
- The analysis of *law-based approaches* vis-à-vis changing technologies and interacting user behavior reveals a set of patterns that guides the legal system's response to change. The default mode, which is currently also at play with respect to privacy issues emerging from Big Data and the Internet of Things, is the subsumption of the new phenomenon under the old (privacy) norms. In some instances, however, one can expect – based on pattern analysis and past experience – more innovative responses by the legal system and its actors, either in the form of gradual adjustments or more radical legal reform. Precursors from the US, Europe and Switzerland have been used to illustrate each response mode.

Considering both the promise and limitations of each approach, the report sketches the contours of a blended governance framework aimed at ensuring the future of privacy in the digitally networked environment. It emphasizes the importance of *legal approaches* – beyond privacy law and including, for instance, consumer protection law as well as competition law, among other areas – but also puts it into a larger perspective of mixed governance approaches that have proven to be most adequate when dealing with the digital environment. Insights from interoperability theory and multistakeholder research might indicate productive *areas for further exploration* when designing for the future of privacy in the digital area, which will ultimately also invite and require a new privacy *ethic* and the development of «Fair Information Technologies.»