Contents lists available at ScienceDirect

Computer Law & Security Review: The International

journal homepage: http://ees.elsevier.com

Paradigm shift

Viktor Mayer-Schönberger

In many ways, it is time for celebration. Four decades ago, on January 28, 1981, the Council of Europe opened Convention 108 for signature.[1] Coming into force in 1985, it was followed by numerous national data protection laws, the European Union Privacy Directive in 1995,[2] and most recently the EU GDPR,[3] giving more than two dozen European nations a single, strong, and enforceable data protection regime that even California is attempting to emulate.[4] The protection of personal data has not only evolved, it seems that it has become a central focus in our hyperconnected world. Decades of conceptual thinking, legislative entrepreneurship and continuous tinkering finally paid off. We may not yet have arrived at privacy nirvana, but we surely seem to have a comprehensive regulatory framework in place.

Away from the self-congratulatory celebrations, however, the harsh reality in our digital age looks much bleaker. Non-democratic nations around the world have realized the power of data and are actively collecting mountains of it on their citizens. Worse perhaps, Edward Snowden revealed a clandestine comprehensive global network of digital surveillance run by governments in Western democracies and orchestrated by the United States, which in an almost Orwellian twist continues to pride itself as the sole beacon of liberty.[5] At least as worrying is the behavior of large digital superstar firms that have built their business models on a blatant disregard for individual privacy rights. Their platforms have become weaponized to unravel not just privacy, but the very fabric of democracy.[6] And even outside of the cabal of digital platforms, no week passes without another large company being implicated in a data leak and shown to be shockingly incompetent guarding the personal data of its customers. For those, who see the privacy glass half empty, there's little reason to celebrate, and much to gripe.

Some proponents of existing data protection and privacy frameworks agree that much still needs to be done, but for them the answer is more of the same: additional and more detailed individual privacy rights, improved enforcement and increased fines. That's precisely the recipe that's been employed over the past decade. Data protection rights got widened, the role of the individual strengthened. We increased our offerings on the altar of informational self-determination, created as a sleight-of-hand by the German Constitutional Court in 1984 to invalidate a rather daft census law.[7] Much like its US counterpart - the mystical "penumbras"[8] of the US Constitution that supposedly protect privacy – "informational self-determination" as a label sounds great (and gelled with the anti-colonial rhetoric of the late 1970s), but lacks conceptual coherence: how can individual humans living social lives be the sole arbiters of personal information?

In its census decision, the German Constitutional Court was deeply aware of the social dimension of information, but unfortunately its more nuanced musings got lost while the short-hand term it created stuck. And over time the term turned into a manifesto. Take individual consent. When Convention 108 was drafted, consent was but one way through which lawful processing of personal data could be enabled; that carried over into many national and European and data protection rules, often with "legitimate interest" being individual consent's powerful alternative. But as the image of an individual's full informational self-determination took hold, individual consent gained currency. To the point that one of GDPR's key changes is the drastic strengthening of the rules governing consent (mostly at the time of collection).[9] Today, in practice consent is often the only way through which legal processing of personal data is perceived to be possible – to the point of absurdity. In my son's elementary school, all parents are by rule members of the Parents Association, but the school has been told by state authorities not to provide the names of parents to the Parent Association without consent. Surely, one would think, there's a legitimate interest of an Association to know the name of its members.

We may long have forgotten it, but there was a good reason that individual consent was just one way to enable lawful processing. In the early days of data privacy laws, the weight of responsibility quite appropriately rested on the processors of data, not on individuals. Only when in the 1970s processing capabilities mushroomed, and ex ante permission systems failed to cope did data protection advocates shift their focus to individual rights in general, and informed consent in particular. It's a bit of an embarrassing birth defect: The individual

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[4] Assembly Bill No 375 (California Consumer Privacy Act (CCPA)), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[5] Edward Snowden, Permanent Record (2019).

[6] See only the so-called Cambridge Analytica case, well explained in the documentary movie "The Great Hack".

[7] BVerfGE 65, 1.

[8] Griswold v Connecticut, 381 U.S. 479 (1965).

[9] Article 7 and 8 GDPR.

https://doi.org/10.1016/j.clsr.2020.105515
0267-3649/

turn in data privacy was born out of a pragmatic need, not rooted in moral principles.[10]

Initially dismissive, data processors have come to embrace the idea of consent. For them, it's a manageable bureaucratic step, with a huge upside: it shifts much responsibility away from them and onto a largely ignorant and impressible individual. With the right wording, we all click "okay" (or at least most of us). The resulting reality of strong individual rights in principle and little accountability of data processors in practice suited advocates of strong privacy laws and processors alike – they both could declare victory – but failed to achieve data protection's goal: to protect us. Researchers muse over what they neatly labeled a "privacy paradox": that individuals care about their privacy when asked but fail to act when it actually matters.[11] But the reason for the seeming paradox may lie less in the twisted mind of the individual, and rather reflect a fundamentally flawed regulatory framework.

Appealing to individual responsibility has had limited effect on everything from limiting smoking to encouraging vaccination. At least since Kahneman and Tversky, we know that humans sometimes make irrational decisions.[12] As social beings, we sometimes need to help each other in our decision making. That's why in many jurisdictions we prohibited smoking in public places, made wearing seatbelts mandatory, and are considering the same on vaccination.

In fact, we deliberately have been *taking away* responsibility from individuals when we cannot expect individuals to have the expertise to make informed and rational choices. Some have, mistakenly I argue, disparaged this approach as "paternalistic", but their ideological bias seems to blind them to the fact that we employ it *all the time*. We do not enter a supermarket with a chemistry lab in tow to test the groceries on offer; we rightly assume that there are processes in place that guarantee the food on display is safe and that supermarkets bear the responsibility to do so. We do not test whether an elevator's emergency brake works before entering it, we assume there's a process in place and that the owner of the elevator is responsible for it. The same is true for cars, planes, drugs, even toys. In fact, the entire system of courts and judges and legal processes is in place to solve conflicts not through the brutal battle of the individuals affected, but by shifting the task to the community – to experts, processes, and clearly defined roles and responsibilities.

In stark contrast, the current data protection regime with its emphasis on informed consent holds mostly us responsible for the protection of our personal data, not those that collect and process it (and reap the economic value from it). At the very least, this is anachronistic – a terribly ill fit between an idealistic idea and the digital realities. We, the people, deserve better.

Don't get me wrong: Like most of us, I *do* believe in the importance of personal privacy. It's not the principle that I am questioning. Rather I suggest that as our digital world has evolved, it exposed an erroneous choice in the mechanism of protection. The focus ought not to be informed consent, which in practice equates to individual responsibility. Rather, we need to hold those that use our personal data accountable. Responsibility needs to rest with those that have a better capacity to understand, foresee, and act. And that reap most of the economic benefit.

Evolving data protection by shifting far more responsibility to data processors and users is not a crazy novel idea. It was a fundamental principle of the first data protection laws.[13] Experts around the world have suggested ways to make it happen.[14] What's needed now is to heed their advice.

The timing may actually be good. After decades of chasing individual consent, it may be time to critically evaluate and look at alternatives. In fact, GDPR itself, the apparent epitome of the individualistic turn in data protection, already includes a number of elements that reflect a turn towards accountability: more effective EU-wide enforcement institutions,[15] a system of severe fines,[16] the permission to repurpose data without consent and to keep it for longer than its original purpose requires,[17] all the way to the renaissance of national data protection regimes for specific types of data use[18] (thereby accepting, perhaps even embracing the regulatory interdependence that may result from it).

Technological development offers a further ground for shifting towards data processor accountability. In earlier days of data analysis, the links between different data elements were given; they were programmed into the processing system. We could correctly claim that algorithms could be exposed and made transparent, and (personal) data was what we needed to focus on. With Big Data and Machine Learning, this is no longer the case. Machine learning means algorithms change every time a new training or feedback data point is evaluated, and the whole system, while being predictive, remains a black box.[19] If not even Google's engineers know what's happening inside one of Google's black boxes, how can we keep alive the pure fiction that individuals do and thus are capable of making well-formed decisions about it?

Regulators and pundits have reacted to the emergence of the black box phenomenon by shifting their focus from data protection to the ethics of data use, "ethical AI" and similar ideas.[20] These ideas may sound powerful and valuable in principle but operationalizing them already turns out to be challenging. Here, the data protection and privacy community have something very important to offer (no, not how to focus on and thus shift the blame to individual responsibility). Rather, the data protection community has developed processes and structures, institutions and networks of expertise that offers rich and eminently useful mechanisms of accountability and responsibility[21]; of assessing, balancing, and mitigating risk; and of establishing instruments of effective control and enforcement. Shifting our data protection focus towards accountability may ensure that this latent privacy knowledge can and will get applied in the context of data-driven machine learning.

There's a final reason, why we should shift to accountability, and it has to do with us. If humans are told that they hold the power in

[10] See only Viktor Mayer-Schönberger, Generational Development of Data Protection in Europe, in Phil Agre / Marc Rotenberg (eds), Technology and Privacy: The New Landscape, MIT Press (1997), 219.

[11] On the "privacy paradox", see Nina Gerber et al, Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior, 77 Computers & Security 226 (2018).

[12] See e.g. Daniel Kahneman, Thinking Fast and Slow (2011).

[13] See e.g. the Swedish Datalagen in 1973.

[14] On the focus on accountability, see e.g. the white papers and reports produced by the Information Accountability Foundation, http://informationaccountability.org/publications/. Suggestions for how fair information processing principles that underly Convention 108, the OECD guidelines and many national data protection laws could be improved to include a stronger accountability and responsibility element, can be found e.g. in Fred H. Cate et al, Data Protection Principles for the 21st Century (December 2013), https://iapp.org/media/pdf/knowledge_center/Data_Protection_Principles_for_the_21st_Century.pdf .

[15] Articles 68-76 GDPR.

[16] Article 83 GDPR.

[17] See e.g. Viktor Mayer-Schönberger & Yann Padova, Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation, 17 Columbia Science & Technology Law Review 315 (2016).

[18] Article 89 GDPR.

[19] See e.g. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (2016).

[20] See e.g. High-Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence (2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[21] For a human-centric history of privacy and data protection, see e.g. Colin J. Bennett, The Privacy Advocates (2008).

theory but in practice realize that they are often the victims, not the agents of change, they rightfully disengage and mistrust data use. Already surveys have shown that much of the data collected in Europe is never even used once.[22] That way, we are foregoing a huge opportunity of learning from data and making better decisions.

But to use data for better decision-making, we need to be able to trust – not us – but the institutions, the processes, the mechanisms of data protection - that they will hold data users accountable. Trust grows with accountability. Without it, on the eve of the 40th anniversary of Convention 108, we may be limping into a new dark age of ignorance.

Declaration of Competing Interest

None.

[22] See e.g. https://blog.datumize.com/evolution-dark-data.