Editorial

In his book *The Craftsman,* Richard Sennett discusses an art that has been mostly lost in modern society: craftmanship. While virtually all products used to be hand-made by guilds, craftsmen and artisans, since the industrial revolution, these processes have been increasingly replaced by machines, triggering a move towards standardisation and mechanisation. Obviously, this has had enormous benefits and boosted both economic growth and individual prosperity. While the carpenter used to work on one table for a year, a factory may produce thousands in one day. And although the bookcase carefully crafted from the finest oakwood could literally last for centuries, a Billy from Ikea is so cheap that replacing it is hardly of any economic concern.

There are, however, also obvious disadvantages. Not only does the trend towards mass production and standardisation bring with it that products are no longer unique, tailor-made for the occasion and personalised according to individual preferences, it also means that the essence and ethics of craftsmanship have waned. What Sennett believes makes a craftsman stand out from any other builder or manufacturer is the urge or even necessity to manufacture not just any product nor to be satisfied with a decent end result, but to strive towards perfection. A craftsman wants to make the best table, produce the finest pottery or create a dress uniquely fit for the occasion, hence the time and effort needed.

Sennett is clear on the fact that mass production and standardisation may have positive effects, even on quality. Some machines may deliver a level of precision that is impossible for a human craftsman to reach or even for the human eye to see. The other way around, what Sennett calls the ‘obsession with perfectionism’ that can occupy the mind of craftsmen can become an obstacle itself or result in imperfect products because all intuition and playfulness is lost. Nevertheless, Sennett sees a number of potential dangers concerned with the loss of craftsmanship. Among the values that are challenged, Sennett especially repeats two throughout his book.

First is the idea or urge of striving for perfection. He describes the amazement of craftsmen from, for example, Japan, a culture were craftsmanship is still highly valued, when hearing the Western idea of quality control and the acceptance of a margin of error. A factory typically accepts that between 1 and 3% of its products has a defect; the costs of removing that margin of error are higher than the costs of replacing the faulty product and the reputation damage combined. But for a craftsman proper, the idea of purposely building in and thus accepting the production of faulty products is something unimaginable.

Second is the idea of the use of minimum force. The craftsman shows his craftsmanship by using the perfect tool for the job and using no more force than necessary. For example,

DOI: 10.21552/edpl/2019/2/3

> chopping food, as in sounding chords, the base line of physical control, the starting point, is the calculation and application of minimum force. The cook turns the pressure down rather than scales it up; the chef's very care not to damage the materials has trained him or her to do so. A crushed vegetable cannot be recovered, but a piece of meat that has not been severed can be salvaged by a repeated, slightly harder blow. The idea of minimum force as the base line of self-control is expressed in the apocryphal if perfectly logical advice given in ancient Chinese cooking: the good cook must learn first to cleave a grain of boiled rice.[1]

Not only is it more efficient and effective to use the right tool and the least amount of force, it is also a matter of aesthetics and a sign of mastery. A chef that uses precisely the right knife and the minimum force necessary cannot only cut a tomato into slices quicker, the end result is also more elegant. In addition, the food sliced with minimum force retains both flavours and healthy ingredients better. A carpenter crafting a kitchen cupboard will use ever more fine tools as the process evolves, careful not to cut out or damage certain parts. Sennett shows that this principle too is challenged by standardisation and mechanisation, among others because most parts for which perfection is needed are removed from the process, because the use of force is no longer a real economic concern and because the ethics and aesthetics of such mastery are no longer valued as they used to be.

In a way, the principles of craftsmanship, the strive towards perfection and the use of minimum force are also the basic principles embedded in law. The necessity principle mandates that force may only be used when necessary, the proportionality principle dictates that the use of force should be proportionate to the goal pursued, the subsidiarity principle stresses when determining the means to achieve the goal, the means for which the least use of force is required should be chosen, all other things being equal, and the requirement of effectiveness mandates that the tools that are used are actually effective in relation to the goal pursued. Parallels may be drawn between the loss of craftsmanship and its ethics and the pressure that is put on these legal principles by modern data-driven technologies.

One of the most interesting debates among data protection experts revolves around efficacy, or the effectiveness of modern data-driven techniques and applications, such as mass surveillance, personalised advertisements and predictive policing. There are a number of reasons why this debate is so fruitful.

First, with these types of modern data-driven applications, it is often very difficult for citizens to demonstrate or substantiate individual harm, precisely because mass surveillance, predictive policing and personalised advertising affect virtually everyone. What harm does it do to a specific person when the intelligence agency monitors the communications meta-data of a whole city? The efficacy debate circumvents this de-

[1] R Sennett, *The Craftsman* (Yale University Press 2008) 167.

bate, or rather, it takes it one step back by turning the table. It is not up to the citizen to demonstrate potential harm, first, it is up to the organisation to demonstrate that it is necessary, proportionate and effective to apply a certain data-driven technology or application. If an organisation cannot prove that gathering data and applying the data-driven technique is at all effective in achieving the goal and that it is more effective than the traditional, non-data-driven approach, it should not use such means out of reasons of effectiveness and efficiency.

Second, it is sometimes suggested that the GDPR and other EU instruments conflict with the so called data-driven era, a world in which everything would be data-based. Some commentators suggest that the GDPR and other data protection instruments go against the grain too much, that they will be unable to stop the inevitable trend of datafication and will thus prove to be nugatory. The efficacy debate challenges such a standpoint by turning the tables: are the technologies and applications that would occupy the data-driven world actually effective; will they even be around in 10 years' time?

Third, and connected to that, when data protection experts are asked to speak on the relationship between privacy and Big Data, the standard frame of the debate is: given the trend of datafication, what conditions can we apply to ensure that privacy and fundamental rights are safeguarded as much as possible. The trend towards a data-driven society is posed as a given and the question whether data-driven techniques actually work is seldom discussed.

Data-driven applications promise benefits in terms of efficiency and effectiveness, leading to a reduction of costs and allowing organisations to pursue their goals optimally. But all too often, these promises turn out to be false hopes.

For example, a living lab project in the Netherlands has received prizes for promoting security in the nightlife area, without there being any data on whether the project has actually reduced the crime rate or the nightlife violence. What the experiment is about is training algorithms to analyse 'screams, noises and sounds' prior to an aggressive event, so that the smart cameras in the nightlife area can analyse potential sounds and inform the police when a noise has been categorised as 'risky'. The question is whether the costs of gathering the data, training the algorithm, doing the experiment, installing the cameras, buying the necessary software and performing the data analytics are lower than simply having two police agents patrol the relatively small nightlife area. This question is all the more pertinent because at this time, the algorithm is relatively bad at making predictions and causes more work for the police, because they have to respond to false positives. Perhaps, in time, these predictions will become more accurate, but even then, police agents are still needed to evaluate situations categorised as risky. In fact, having police agents patrol a nightlife area might have a higher preventive effect than smart cameras and has the additional benefit that it creates trust in law enforcement authorities.

Another example might be the fight against doping in sport. Doping is used by only a very small portion of athletes: steroids and related products are used by amateur body builders and professional top athletes sometimes use products such as EPO. The latter category is limited to athletes performing in a small number of sports, such as cycling, track and field, rowing and other endurance sports. Nevertheless, doping authorities claim testing authority over practically all athletes, amateur or professional, chess player or cyclist, meaning that they can test about 1/3 of the total population of a country. Doping tests can be quite intrusive and rather than using targeted measures against specific athletes, the World Anti-Doping Agency has set up a sort of mass surveillance system in which all athletes can be tested at random, without any suspicion. Most tests are conducted either by collecting the urine of an athlete, for which a doping agent has to be present in the room closely watching the genitals of the athlete, or by blood controls, for which a doping agent has to insert a needle in the athlete's body to extract blood samples. Testing figures of 2015 showed that of the more than 20,000 blood samples taken, only five cases led to the establishment of a direct doping violation.

These two anecdotes certainly do not prove that data-based technologies and applications do not work. But they do illustrate that both private and public agencies tend to start large scale data-driven projects without much evidence for their presumed efficiency of effectiveness. Organisations are becoming more and more like the novice carpenter with a preference for the sledge hammer. I could easily give a number of other illustrations to make the point briefly.

The effectiveness of mass surveillance used by intelligence agencies, wherewith they gather and analyse huge amounts of meta-data, for preventing terrorism has not been proven. Both defenders of privacy, such as Edward Snowden, and experts that do believe in the benefits of certain forms of meta-data analysis, such as Bill Binney, a former high placed official at the NSA, believe that mass surveillance is wholly ineffective. Snowden is convinced that intelligence agencies gather the data for other purposes, such as diplomatic and economic espionage. Binney, who wrote a foreword[2] in one of the previous editions of EDPL, suggests that intelligence agencies pollute data-profiles by gathering too much data with no or low significance. NSA director Keith Alexander said in 2013 that no less than 54 terroristic attacks were prevented based on the NSA's surveillance programs.[3] But an independent study showed that it was more likely that only one potential domestic suspect of plotting a terroristic attack was brought to light through the data analytics program.[4] The question is whether it would have been more effective to invest the billions of dollars that now went to the NSA in more traditional means of fighting terrorism, such as infiltrating terrorist networks.

Given the secretiveness of intelligence agencies, it is difficult to answer that question and assess the effectiveness of mass surveillance programs. But there are data on the

[2] William Binney, 'Big Data Analysis' (2017) 3(1) EDPL 13-15.

[3] NSA, 'Speeches and Congressional Testimonies' <https://www.nsa.gov/news-features/speeches-testimonies/Article/1620137/remarks-by-gen-keith-alexander-commander-us-cyber-command-uscybercom-director-n/> accessed 20 June 2019.

[4] Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' (23 January 2014) <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf> accessed 20 June 2019.

use of a similar technique by law enforcement agencies, namely predictive policing. The philosophy behind predictive policing is that law enforcement agencies gather data about crimes - when they have been committed, where, by whom, against whom, why, how, etc - and that an algorithm can predict on the basis of these data where a crime is likely to happen or what the likelihood is that a particular person would commit a crime. There have been many reports about the use of predictive policing in the USA and the UK, which were among the first countries to deploy this technique. The reports suggested that, even leaving aside the dangers for privacy, discrimination and the potential negative effects on the right to a fair trial, such techniques are simply not effective. In the Netherlands too, a pilot was evaluated by the Police Academy, part of the police organisation, and the conclusion was simple: 'We did not find any indications that predictive policing would eventually lead to lower crime rates.'[5]

In the private sector as well, there is a substantial number of failures when it comes to such techniques and applications, though the general public is often not informed of the fact that a year or two years after the introduction of a data-driven project, a company puts it on hold due to the lack of success, because private organisations rather keep certain failures behind closed doors. Even those companies that are seen as market disrupters, such as Space X, Uber and Tesla have never made a profit. Obviously, companies such as Google and Facebook make money, primarily through offering personalised advertisements. Interestingly, even with these types of advertisements, there is hardly any evidence to suggest that they are actually more effective than contextual advertisements, which are based on the context, such as the website that the user visits. An example of contextual advertising is when an advertisement for a football ticket for the next match of Bayern München is shown to a person that is looking at a news item regarding the last match of this football club on the website of the Süddeutsche Zeitung. For contextual advertisements, no personal data are required.

Likewise, the effectiveness of other data-driven applications has been called into question. For example, when introducing Google Flu Trends, Google claimed that is was able to predict with 97% accuracy, based on the search queries by users (eg 'coughing', 'headache', 'doctor', etc) when and where the flu would break out. However, subsequent studies showed that Google was actually structurally incorrect in its predictions and suggested that at most, using Google Flu Trends data in combination with historic flu levels, the number of errors in predictions could be reduced by some 10-15%.

What do we learn? Certainly not that data-driven technologies do not work nor that we should not invest in them. To be sure, some data-driven technologies will work and some of them will have so many benefits, that we would take the potential downsides for granted. Other projects, however, will prove to be ineffective. The point is: we don't

[5] Bas Mali, Carla Bronkhorst-Giesen and Mariëlle den Heng, 'Aanwijzingen dat predictive policing uiteindelijk leidt tot minder (stijgende) criminaliteit hebben we niet kunnen vinden.' (Politieacademie, February 2017) <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.PDF> accessed 20 June 2019 (in Dutch).

know which data-driven technologies will work and which will not. It seems that rather than going along with the frame of 'the data-driven environment is here to stay, how do we reconceptualise fundamental rights in order to fit the new reality', it is pertinent to ask first 'will the data-driven environment actually be here to stay, which data-driven techniques are actually effective, etc?'

To avoid costs and unnecessary data gathering, data-driven projects should only be introduced if there is reason to believe that they will enable organisations to operate more efficiently and effectively than through non-data-driven operations and that the costs of introducing and operating the data-driven technologies are lower than the potential gains. Both the European Parliament and national parliaments, when discussing new data-driven technologies often forget to ask these simple questions. In addition, when introducing such new technologies, a sunset clause could be built in. The government should do a baseline measurement of how effective the operations are before the introduction of the data-driven technology, which benefits in terms of effectiveness and efficiency it believes the data-driven technology will have and finally, evaluate whether the technology actually delivers on its promises. If, after two or three years, there appear to be no or only marginal gains, the data-driven technology should be stopped.

Let me now introduce this edition of EDPL.

We have the great honour of featuring an opinion by Antoine Picon, Professor of History of Architecture and Technology at the Harvard Graduate School of Design. His work on smart cities and architecture is highly recommended. The second opinion is by Esther Keymolen, an international expert on the relationship of trust, privacy and technology. Both discuss the implications of smart cities and the role and rights of citizens in such environments.

There are five scientific articles included in this edition, four of which regard the medical domain. Theo Hooghiemstra discusses the right to informational self-determination in the health sector, Daniel Jove sheds light on the implications of the *Nowak* case for subjective comments in a medical history, Paola Aurucci delves into the impact of the GDPR on Italian biomedical research and Trix Mulder gives an historical overview of the evolution of the protection of data concerning health in Europe. Finally, Julian Hölzel discusses the notion of differential privacy.

We have four reports in the section led by Mark Cole. Christina Etteldorf has written two of them, one on the EDPB's take on the interplay between the ePrivacy Directive and the GDPR and another on the German Competition Authority's actions on Facebook's data usage. In addition, Päivi Korpisaari has written a report for our GDPR Implementation Series, covering Finland and Sören Zimmermann gives a comparative overview of Israel's data protection framework.

The Case Notes section, led by Maja Brkan and Tijmen Wisman, contains three case notes. First, Eleni Kosta and myself have discussed the *Big Brother Watch* case of the

ECtHR. In the annotation on the *ML and WW v Germany* judgment, Elena Corcione discusses the ECtHR's approach to questions revolving around the right to be forgotten. Marc Rotenberg and Bilyana Petkova have shed light on the US case *Airbnb, Inc, and HomeAway.com v City of New York*. Here a New York ordinance requiring home-sharing companies to provide monthly records containing personal information of the companies' users was deemed to be an unreasonable search and seizure within the meaning of the Fourth Amendment.

Finally, the Book Reviews section, led by Gloria Gonzalez Fuster, contains two book reviews. Elisa Spiller evaluates Van Alsenoy's book *Data Protection Law in the EU: Roles, Responsibilities and Liability* and Gloria González Fuster herself discusses Woody Hartzog's *Privacy's Blueprint: The Battle to Control the Design of New Technologies*.

For those interested in submitting an article, report, case note or book review, please e-mail our executive editor Nelly Stratieva (<stratieva@lexxion.eu>) and keep in mind the following deadlines:

- Issue 2019/3: 15 July 2019;
- Issue 2019/4: 15 October 2019 (Young Scholars Award);
- Issue 2020/1: 15 January 2020;
- Issue 2020/2: 15 April 2019.

I hope you enjoy reading this edition of the European Data Protection Law Review!

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, Netherlands