Editorial

The relationship between data protection, power and truth will be an increasingly important concern. As is often pointed out by scholars these days, perhaps the ultimate value undermined in Orwell's *1984* was not privacy, but truth. It is the *Ministry of Truth* that exerts control over information flows and news. Winston works at the department were historical records are 'rectified' so that the official chronical of what had happened aligns with what the state believes should have happened. The ultimate goal is to erase any sign of divergence from the official party line; divergence does not exist and therefore cannot be thought – divergence cannot be thought and therefore cannot exist. The *Thought Police* persecutes people when individual and independent thinking occurs, which is considered a *thoughtcrime, doublethink* means that seemingly contradictory information can be true at the same time and the party has introduced a new language, which is called *newspeak*. Control over language, thoughts and truth are omnipresent in Oceania.

Interestingly, truthfulness is an essential, but difficult to grasp element in the General Data Protection Regulation (GDPR); correctness, integrity and integrality are core values that are protected through a number of provisions. One of the core data protection principles is that of data accuracy, as contained in Article 5 paragraph 1 sub (d), which specifies that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken by the data controller to ensure that personal data which are inaccurate are erased or rectified without delay. In addition, the requirement for the data controller to keep records and to communicate to the data subject where the data in its possession originate from, as per Article 14 paragraph 2 sub f, allows for action at the source when an error has been established.

Many of the data subject's rights can be understood in relation to truthfulness as well. Obviously, Article 16 contains the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data. It even stresses that, taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. The latter element is interesting, because it gives a right to the data subject to ensure not only that the data controller processes correct data, but also that it processes all relevant data. Article 17 grants the data subject the right to obtain from the controller the erasure of personal data without undue delay when processed contrary to the GDPR, albeit a (large) number of exceptions exists. Article 19 requires the data controller to notify other data controllers, that have copied the data, of the fact that the data need to be rectified or deleted according to Articles 16 and 17 GDPR. This ensures that the digital records are harmonised; no two versions of the truth can co-exist. Finally, mention should be made of Article 22, which essen-

DOI: 10.21552/edpl/2019/1/3

tially holds that a data controller must always assess whether the general profile he has made also applies to the specific case or person at hand. Recital 71 clarifies that the data controller should do its best to ensure that 'that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised'.

The question is of course who ultimately decides on issues of correctness, integrity and integrality. The data subject, the data controller, the state?

An opening was provided in the well-known *Google Spain* case, in which information about a person's financial malaise that had occurred decades ago was digitalised and published online by a newspaper and could be found in the top list of Google's search results when entering that person's name.[1] The European Court of Justice did not find that the newspaper shouldn't have written the story or shouldn't have published it online, but turned to Google. Although the Court essentially judged this case under the data minimisation and storage limitation principles, stressing that the processing of these data was not necessary, proportionate and no longer relevant for the purposes for which they were collected, perhaps a reference to the data quality principle would have been more appropriate. The problem was not so much that details about the person's history were recorded and made available; the problem was that this information appeared on top of Google's search hits. If Google is seen as providing a digital biography about a person, the problem was that this biography was outdated and incomplete. If the search hit had been indexed as number forty-something, the Court of Justice would probably have reached a different conclusion. In the end, it was the lack of new information about the person's life after that event that did injustice to the person. His digital biography had been narrowed down to one juicy detail. This raises the question to what extent data controllers should have the obligation to ensure that the digital biography is not only correct and up to date, but also complete.

There are also instances where inclusion of historically correct data will be problematic as such, although this will typically also concern cases in which one specific detail might overshadow all other biographical details, either on a legal or a societal level. Examples may be a criminal record or an experimental phase during adolescence. Certain poignant facts may be so spectacular and appealing to the imagination that others have the tendency to refer to that one biographical detail to determine a person's identity. This not only narrows a person down, but also limits a person's capacity to develop into a new direction; the idea behind the possibility of a clean slate and the right to be forgotten is based on the belief in a second chance. Again, it is difficult to ascertain how the relationship between data protection, power and truth should be crystalised on this point. On the one hand, the truth about a person's past should not determine the truth of his future – an offender needs to be free from constant reminders about his criminal past to get a job, develop a social life and break with a criminal milieu. On the other hand, clean slates should not mean that history repeats itself. Vic-

1 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317.

tims of crimes often say that they have been treated unjustly, because they were not treated as a human, but narrowed down to one specific aspect – their body, their money, their race.

A perhaps even more difficult question arises when a person no longer wants to be reminded of a particular aspect of his past, because he is ashamed of it, because he no longer identifies with the image of his past self. Should a person have the right to delete images of him as guru of a religious sect because he has renounced his previous religious beliefs? Should that person not rather accept that he is the person that used to be religious and now no longer is, rather than the person that is not religious? And what about a person who wants to delete all photos of him and his ex-lover. Obviously, identities and our personal narratives depend on selecting certain information over others – we cannot see ourselves as a mere bundle of facts. We have to prioritise certain information over other and even tend to delete or disregard information about ourselves that conflicts with our dominant understanding of ourselves. In a way, the law tries to mirror the situation before the data-driven technologies had entered into our world. There used to be very few data and records about a person's past. The information about a person that was available was 'stored' in the memory of the people, which made it both subjective and contestable, and meant that it was ultimately possible for a person to avoid the data by relocating to another part of the country or the world. A person could create a new life, a new truth, a new personal narrative. Whether the law will succeed in transposing this pre data-driven world social practice to the data-driven world remains to be seen. Perhaps there are other ways to form and shape identities?

These examples show that there might be a discrepancy between (data about) a person's past and a person's current identity. Equally, there can be tensions between data about a person's current life and what he identifies with. The most awkward examples of this tension are instances in which another knows more about us than we do. Such may relate to a company knowing about a person's pregnancy before she does and informing her through pregnancy-related advertisements. Alternatively, companies like Facebook may infer a person's sexual preference from data about his music taste, friends and fashion statements and confront an adolescent that may still be unsure or feel insecure about his sexual preferences. Although the data might be true, the information is so relevant to our identity and the perception of ourselves, that being informed about pregnancy, sexual preference or other highly personal aspects by others can mean that a person is deprived of the possibility to write his own biography, develop his own personal narrative and exert control over who he is.

Another issue is the question of what should be considered correct information. A person may be a man biologically and legally speaking, but self-identify as a woman. Facebook might think a person is gay or right wing, while that person may consider himself straight and progressive. Can a data subject invoke Article 16 in such instances and should the data controller always follow how a person self-identifies? Should a judge ultimately determine what is biographically correct information and what would that require from the data controller and the data subject in court? That the data con-

troller 'proves' why it thinks a person is gay, male or right wing; should the data subject demonstrate that he really is not? Both could lead to uncomfortable situations.

Another question that can be raised about the relationship between data protection, power and truth relates to judging a person on the basis of presumed and probabilistic facts. Profiling is increasingly used, inter alia, by banks, health insurers and law enforcement authorities. Typically, such predictions are based on statistical correlations – 60% of the heavy smokers may develop a certain disease, 40% of the people living in a certain neighbourhood may not repay their loan, 15% of the people with a certain background may be inclined to recidivism. Organisations have always operated on the basis of predictive profiles; the core business of banks and insurance companies is precisely to calculate risks and potential damages. It would be too tedious to do an individual risk assessment on each and every specific person or case. Article 22 GDPR, however, prohibits automatic decision making when this has significant effects on a person; there should always be a human that evaluates the applicability of the general profile on the specific person. But how far should such an evaluation go; how much effort should the data controller put into assessing the validity of the general profile in a specific case?

A final difficulty that the GDPR signals is the completeness of information stored by data controllers. Suppose a bank would make a risk profile of a person based on a small set of data, and derive from data-analysis that that person is untrustworthy or falls within the high-risk category. Can the data subject, relying on Article 16 GDPR, provide additional information about his trustworthiness to the bank and to what extent should the bank be required to take such information into account? And what about the case discussed in *Google Spain*: can a data subject require of Google that it indexes new information provided by him or puts the newest and most appropriate information on top of the list? Can the data quality principle be extended to mean that the data subject has the right to demand of the data controller that it takes into account all information he feels is relevant for assessing him?

In brief, the data quality principle will play an increasingly important role in the data-driven environment and might become a pivotal tool for writing one's personal narrative and developing one's own identity in a world of abundant data about a person's past, present and future. Putting more emphasis on data quality, integrity and integrality would not be a novelty, but rather reconnect with the original rationale behind the data protection rules. The first sentence of the first article of the first European-wide data protection instrument, the Resolution from 1973 from the Council of Europe (CoE) on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, held: 'The information stored should be accurate and should be kept up to date.'[2] The most fundamental principle of data protection is perhaps the data quality principle.

2 Council of Europe, Council of Ministers, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

This edition of the European Data Protection Law Review has a lot to offer. We begin with two opinions, by Anita Allen, professor of Law and Philosophy at the University of Pennsylvania, and Deni Elliott, professor for Media Ethics and Press Policy at the University of South Florida, who reflect on the relationship between law and ethics in the field of privacy and data protection.

In the Articles section, we have five highly interesting papers. The first by Federike Zufall provides a counter-perspective to the right to be forgotten in the form of the right to know. Matthew White discuses immigration in the light of the European Convention on Human Rights; it provides an interesting insight in the interrelationship of EU, CoE and UK law in the domain of data protection and security, complicated even further by the Brexit. Leading a group of authors working at Department of Population Health of University of Oxford, Jessica Bell and her co-authors discuss the tension between public interest research and data subjects' rights. To what extent can the latter be legitimately curtailed when necessary for the former? Sara Leonor Duque de Carvalho discusses the relationship between Convention 108 of the Council of Europe and the GDPR of the EU – is it enough for a country to implement the Convention in order to be considered a country with an adequate level of protection under the GDPR? Finally, Sheng Yin Soh proposes a soft paternalistic approach through the use of 'privacy nudges' as an alternative regulatory tool to informed consent to nudge users towards more optimal privacy protection decisions.

As always, the Reports section led by Mark Cole is one of the features that make this journal stand out. This edition contains a report by Jan Henrich, who discusses the recently published Guidelines to respect, protect and fulfil the rights of the child in the digital environment by the Council of Europe; Olivia Tambou discusses the first post-GDPR fines of the CNIL against Google; Christina Etteldorf analyses the guidance given on direct marketing by the German Data Protection Authorities; Hitomi Iwase provides an overview of the Act on the Protection of Personal Information in Japan; and Eleni Kyriakides discusses the implications of the Clarifying Lawful Overseas Data (CLOUD) Act, that was signed into law in the United States March 2018. In addition, there are two reports in the Practicioner's Corner. Wang Lei provides an overview of Data Utilisation Disputes in China and Sjoera Nas assesses the risks of using Microsoft Office ProPlus.

The Case Notes section, led by Maja Brkan and Tijmen Wisman, contains three annotations. Katrien Keyaerts analyses the case *Ben Faiza v France* by the European Court of Human Rights, *Ministerio Fiscal* by the Court of Justice of the European Union is discussed by Xavier Tracol and comments on the Opinion of Advocate General Szpunar of the Court of Justice in the case of *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* are provided by Alberto Miglio. Finally, Gloria Gonzalez Fuster, the editor of the Book Reviews section, has invited Olga Gkotsopoulou to write a book review of Simon Davies' personal chronicle; Laura Drechsler has discussed the edited volume on *Privacy in Public Spaces*, edited by a research group of the Tilburg University, namely Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops.

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

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