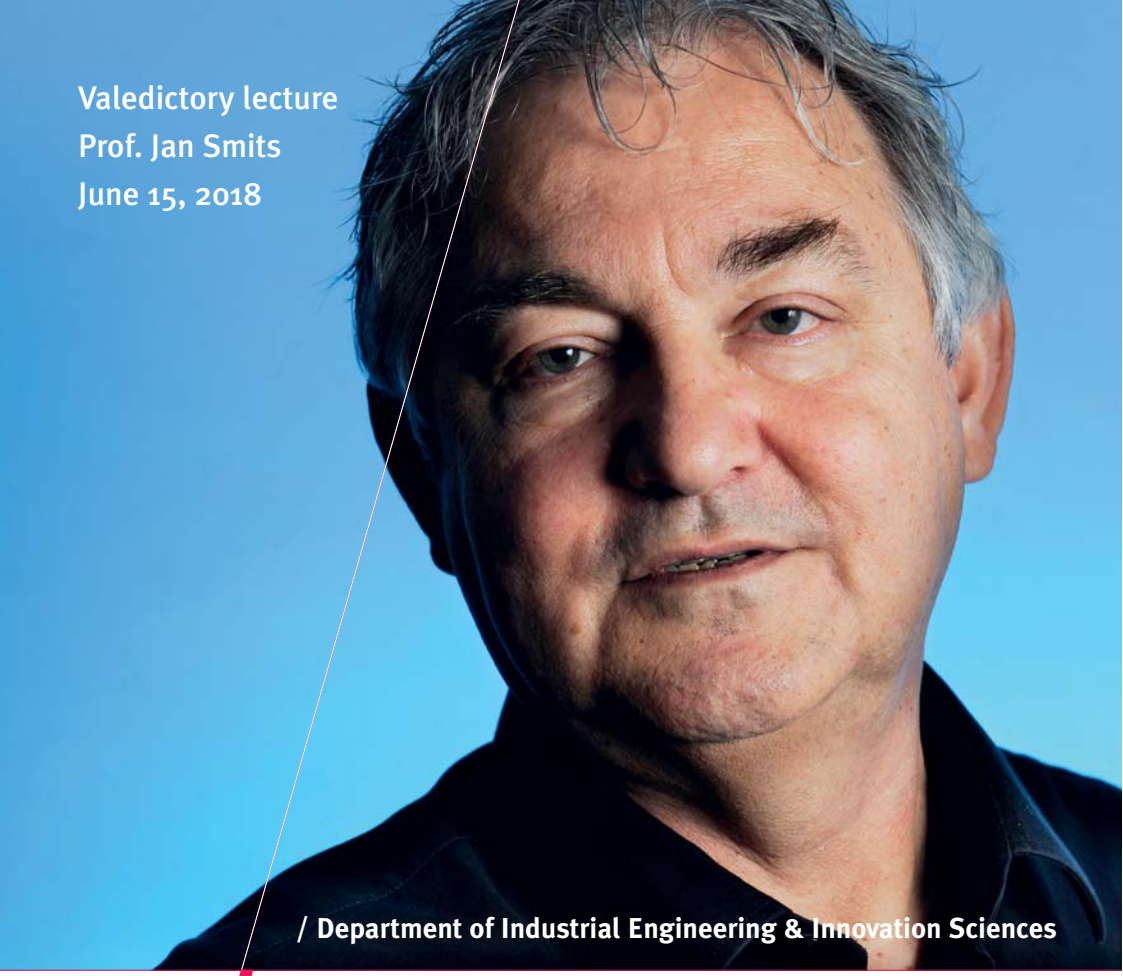
Innovation: less jurisdiction and human dignity?



Valedictory lecture
Prof. Jan Smits
June 15, 2018

/ Department of Industrial Engineering & Innovation Sciences

TU/e Technische Universiteit **Eindhoven** University of Technology

Innovation: less jurisdiction and human dignity?

Where innovation starts

Valedictory lecture Prof. Jan Smits

Innovation: less jurisdiction and human dignity?

Presented on June 15, 2018
at Eindhoven University of Technology

Introduction

Combining Law and Technology (mainly due to ICT) is a multidiscipline that is difficult and hard to market. I would argue that it is of great societal value. Usually, academics trained in law are not very familiar with technological developments and the other way around, engineers are usually not very familiar with legal rights and obligations (maybe apart from understanding how much salary the university and or employer should pay).

25 Years and 4 days ago I was standing at this exact same spot to give my inaugural address.[1] Today, officially concluding my academic life, I will address three subjects that, in my view, demand the cooperation of both lawyers and engineers. Established fora for such a meeting ground are standardization organizations. First, I will describe why the (group of) standards known as Content Delivery Networks and Digital Object Architecture challenge our basic legal notion of being the master of one's territory, for what the law calls 'jurisdiction'. Second, I will deal with the notion of informed consent, which is supposed to allow us to be the master of our data and of what data we share with others. Third, I will touch upon the developments in Artificial Intelligence that challenge law as well as technology. Before that, I need to say a few things on standardization processes and outcomes.

Types of standardization

Standards are developed and come into effect in many different ways. Looking into the organizational side of standards, it is common to make a division between formal and informal organizations. Formal standards stem from Standards Development Organizations (SDOs), and their standards are approved or adopted by one of the national, regional or international standards bodies. Informal standards are developed and published by organizations and/or consortia, e.g. IEEE (Institute of Electrical and Electronic Engineers), SAE (Society of Automotive Engineers) and SEMI (Semiconductor Equipment and Materials International). Private standards are developed for internal use by companies.[2]

Two of my PhD students reflected on different aspects of the process of standardization. First, Rudi Bekkers studied the success of European mobile telecommunications standards, and he became a full professor on Standardization and Intellectual Property at my capacity group in November 2017.[3] Second, Andriew Lim studied what the role of negotiations and pre-standardization activities were in determining the outcome of standards with regard to mobile payment, Andriew is now Lector Technopreneurship and Innovation in Hospitality at the Hotelschool The Hague.[4]

Proprietary standards, CDN's & DOA

To allow the appropriate functioning of networks, the network needs to know where the information that is being searched for, is located. For example, to allow telephone calls to be made, the network needs to know where the other telephone is. To show a requested webpage, the internet needs to know where that website is. The solution is to create an address and delivery system. In the mobile network, the address is countrycode-telephonenumber, +31 123456789; on the internet it is the Unique Resource Locator (URL). But with the networks growing more and more together, they converge, and therefore a solution is necessary to be able to address any device and/or file on whatever network available on the globe.[5]

To identify a mobile telephone knowing the assigned number is enough (technically speaking a lot of agreement and standardized requirements are necessary 'under the hood') to enable the connection between two telephones. The same applies for connecting two computers on the internet – there is the DNS name such as www.tue.nl. The network standards and naming systems allow connection to the TU/e website from www.eindhoven.nl or any other website on the globe. The different networks (mobile, broadcast, internet, etc) are converging whereby the smartphone is nowadays the most commonly used access tool. At the same time the amount of data that needs to be transferred over all the networks is growing rapidly, see Figure 1.

This also means that each individual smartphone is uploading and retrieving more and more data. To prevent smartphone users having to wait unreasonably long for the requested video or other data, several technologies have been developed to enable the delivery of data-intensive content.

Proprietary Standards

Tech companies such as Google, Apple, Facebook and Amazon (in EU jargon sometimes referred to as GAFA)[6] are so strong that they can develop their own content delivery networks. These networks allow data-intensive content to be delivered to the user without almost any delay, thus creating an excellent user experience. As these networks are based on proprietary standards, other parties cannot use or have access to the technology. The GAFA firms are now also building

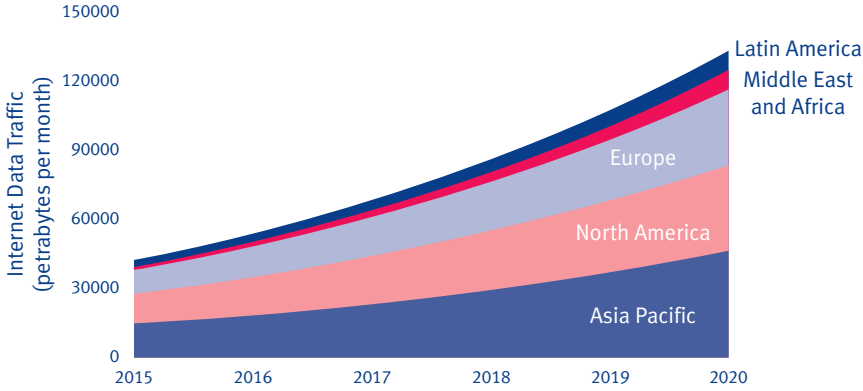


Figure 1
Global Consumer Traffic Forecast (source Cisco 2016)

their own global internet infrastructure by laying proprietary submarine cables.[7] The result of these two developments is that they are very close to being physically and jurisdictionally completely autonomous, elusive and untouchable.[8] So from a legal perspective, content delivery through these proprietary networks is being done irrespective of jurisdiction.[9] Serge Gijrath, one of my PhD's, advocated the use of contracts instead of governmental control over connecting different networks. He now holds a chair of telecommunications law at Leiden University.[10]

CDN's

As a counterweight to these proprietary standards, telco firms and router and switch providers therefore started their 'own' standardization of (the now capitalized) Content Delivery Networks (CDN's) in order to deliver the same type of service but chose to go through the normal standardization development. The European Telecommunications Standardization Institute (ETSI) is then an appropriate organization, due to its multi-stakeholder participation from industry, academia as well as governmental institutions. ETSI can and will facilitate such a standardization development.[11]

> Most CDN providers will provide their services over a varying, defined set of PoP's, depending on the coverage desired, such as the United States, International or Global, Asia-Pacific, etc. These sets of PoP's can be called "edges", "edge nodes" or "edge networks" as they would be the closest edge of CDN assets to the end user.[12]

As already stated, CDN technology is allowing for an almost immediate response to a user reaction on the internet. CDN's facilitate content consumption irrespective of the platform and device the user is using. At the beginning of this century, one could not access the Internet with a mobile phone. Nowadays using your phone is often more convenient than using your PC. A mobile phone was not able to access broadcasting networks, nowadays you can watch the ten o'clock news on a mobile phone, as well as the latest Hollywood blockbuster. The standardization of these different platforms, such as mobile or broadcast networks, have traditionally followed different paths, so they did not interoperate across different platforms.[13] Content Delivery Networks (CDN) offer the end-users fast access to media content by optimizing network resources. Proxy-servers, all holding the locally most sought-after content, are placed close to the physical location of large user groups. From a legal perspective, content delivery through CDN's is being done irrespective of jurisdiction, or phrased differently, wherever the user is and without the user knowing where the information is coming from.

DOA's

A development that is in complete contrast to proprietary content delivery and CDN's is the so-called standardization of Digital Object Architecture (DOA).[14] It is an architecture that no longer allows the identification of the machine (that would normally be replaced every five years on average) where the information could be found, but an architecture that identifies information represented in the form of persistently identifiable data structures called digital objects, and, by giving each a separate identifier, every digital object is uniquely identifiable.[15] Although it might be necessary from a technological point of view to let the internet keep on functioning also in an era when IoT devices are being added exponentially, it allows for control of the (users of these) devices, which is very scary from an open democratic society viewpoint. The ultimate consequence is namely that each device, credit/debit card, bank account, mobile phone, laptop, iPad, Apple watch, fitbit, smart meter, WiFi connected scales and toothbrushes, smoke detectors, and each file, document, photo, video available on that device will have an identifiable owner. This always allows individual identification, making mass surveillance a piece of cake.[16] It is therefore not strange that during the World Telecommunication Standardization Assembly held in Tunisia in November 2016, countries such as Russia, China, Iran agreed on the DOA standard in the International Telecommunications Union (ITU) environment known as X 1255.[17]

Recommendation ITU-T X.1255 Framework for the discovery of identity management information
The purpose of Recommendation ITU-T X.1255 is to provide an open architecture framework in which identity management information can be discovered. This IdM information will necessarily be represented in different ways and supported by various trust frameworks or other IdM systems using different metadata schemas. This framework will enable, for example, entities operating within the context of one IdM system to have identifiers from other IdM systems accurately resolved. Without the capability for discovering such information, users and organizations (or programs operating on their behalf) are left to determine how best to establish the credibility and authenticity of a suitable identity, whether for a user, a system resource, information or other entities. Based on this information, it is up to the user or organization to determine whether or not to rely on a given trust framework or other IdM system for such purposes. The core components of the framework set forth in this Recommendation include: 1) a digital entity data model, 2) a digital entity interface protocol, 3) one or more identifier/resolution systems and 4) one or more metadata registries. These components form the basis of the open architecture framework.[18]

Despite warnings from different corners, one of them being Anthony Rutkowski[19] a long time and renowned connoisseur of the ITU, the meeting put the proposal forward to the plenipotentiary conference of the ITU in 2018.[20] It is not just this standard (X.1255) that these countries put forward, the development of the ITU being a less neutral UN Specialized Agency already started in the early 2000s. This cumulated in 2012 when the ITU held its plenipotentiary conference in Dubai and approved a resolution that stipulated that each individual country has an **equal role and responsibility** over the (whole) internet. In the wording of the resolution: '(...) *all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized*'.[21]

Some observations concerning network standards

Our ability to use the law as a means of finding out whether some companies or even countries overstepped their attributed powers is growing ever more difficult. First, proprietary network standards can be used to disable 'the location from the service provision' (see the equivalent of nations not knowing how to tax these tech giants in an attempt to get some form of tax control over them the EU commission has launched a proposal)[22] and, second, our data are becoming vaporized in a cloud environment that has no location and, consequently, our personal data also have no location and thus no jurisdiction. Having no jurisdiction means having no means of legally contesting a contract, a consent, a cookie policy, etc. In those

circumstances there are no rights and obligations, either for me as a user or for the service provider because there is no (physical) location, and therefore no known jurisdiction.

So, either we lose grip on how and what content is being delivered to my terminal equipment through a proprietary content delivery standard over privately owned submarine cable systems or we allow for a potential authoritarian[23] grip on all available interconnected files (and devices) in use by every citizen of the world. In my view these developments (proprietary standards, CDN's and DOA's) are threatening democracies. Paradoxically the DOA system could be used to enhance EU jurisdiction and give the Union a primary place in the Handle system so that EU jurisdictional power can be upheld easier. On the other hand, it can also be used in the hands of authoritarian regimes to strengthen their grip on knowing everything of its citizens.

It is especially here that law and technology and lawyers and engineers need to understand each other and work together to help foster democracy and its underlying respect for human rights. In 2010 a doctor's degree was granted to one of my PhD students, namely Hans Fischer (nowadays a math's teacher at Vossius Gymnasium, a secondary school in Amsterdam) for his provision of a test to allow for the determination whether traffic data (that is produced in abundance in CDN/DOA enabled networks) is eligible for human rights protection.[24] Notably traffic data (often referred to as meta data) is very telling on who and what we are as human beings. It needs a joint effort from engineers and lawyers to 'fight' against this potential loss of democracy and human rights.

Privacy

The German Bundesgerichtshof (Leserbrief) acknowledged in 1954 that individuals have a fundamental right to *Menschenwürde*, human dignity.[25] The judges derived this right from the right to privacy and the right to develop one's personality. The objective of this *human dignity* right is to adequately protect the attributes (including the data collected) of the human person and including the right to control one's personal data as part of the right to privacy, in order to protect against all kinds of violations of one's personality. Human dignity usually manifests itself in this personality right. The merits of the Leserbrief case lie in the fact that the general personality right and human dignity are inextricably intertwined.[26]

The European Union has included human dignity in its laws, thereby acknowledging the importance of this right. The first Article of the European Charter of Human Rights states that *"Human dignity is inviolable. It must be respected and protected."* When the merits of the Leserbrief case are applied in the context of Union law, it could be argued that a European personality right exists, because human dignity is recognized within the Union. In the Omega case the European Court of Justice recognized human dignity as a general principle of Community law.[27] We can therefore conclude that human dignity functions as the foundation of the personality right because having human dignity implies a personality right; collecting data on a person by internet service providers needs to be seen in the context of human dignity.[28]

To understand privacy as a concept, one of my former PhD students B.J. Koops,[29] nowadays a full professor of regulation and technology at Tilburg University, has won a NWO grant allowing him to study (the concept of) privacy. About a year ago his research group published *A typology of privacy*.[30] In this publication they make clear that there is no one dimension to privacy. Privacy protection needs to be understood in a very private almost physical way when dealing with data surrounding our body, extending it to the place where we live and stay as well as walking along the street. The publication distinguishes 8 different dimensions/spheres and a single all-encompassing one, namely informational privacy (see Figure 2).

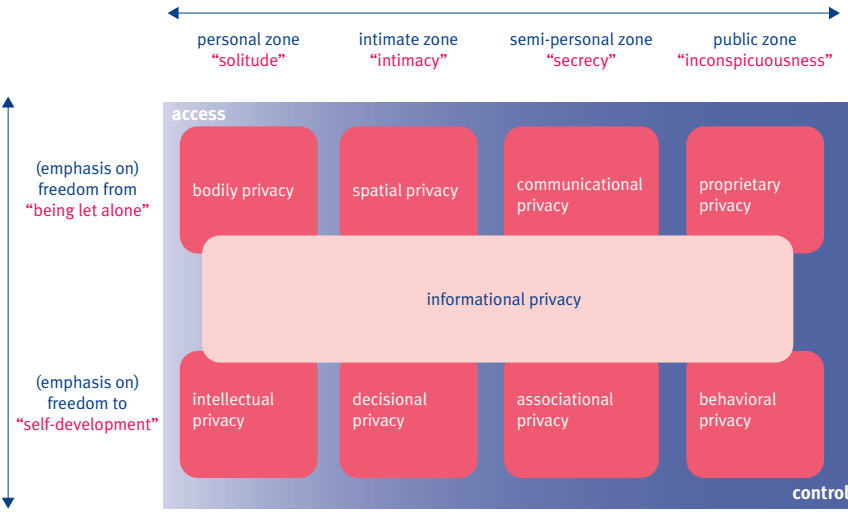


Figure 2

Koops's Typology of Privacy

Informational privacy, i.e. privacy concerned with the collection of data in all kinds of different spheres in which we as humans 'are' and/or 'operate'. The merits of this research are that we, both engineers as well as lawyers, can appreciate the enormousness of the data collection that surrounds us as we increasingly become part of a datasphere.[31] Often, we approve the collecting of (personal) data involving all these spheres/zones. So, it is necessary to analyze how the newly applicable EU General Data Protection Regulation (GDPR)[32] cites our approval through the informed consent requirements. I will try to show that although the idea underlying informed consent seen from the legal requirements is sound and necessary, unfortunately it is not going to make our consent more informed.

Informed Consent[33]

The idea underlying the GDPR concerning informational privacy is that people are invited (seduced)[34] to accept a data processing operation, and as such this invitation and subsequent consent should be subject to rigorous requirements. The GDPR is aimed at protecting the fundamental rights of data subjects.[35] The controller wishes to engage in a processing operation that would be unlawful without the data subject's consent. The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of data processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data were based on consent of the data subject, this would not legitimize collection of data which is not necessary in relation to a specified purpose of processing and is fundamentally unfair.[36]

Pivotal to the informational privacy is the collection of personal data, and whether we have given our informed consent. Informed consent is one of six lawful bases to process personal data, so says Article 6 of the GDPR. Let me mention the other five before I go into more detail about Informed consent. Processing shall be lawful (1) only if necessary for fulfilling a contract, (2) as a consequence of a legal obligation a controller has to comply with, or (3) when the processing is necessary in order to protect the vital interests of the data subject or of another natural person, (4) in case a task is carried out in the public interest or in the exercise of official authority vested in the controller, (5) when the controller/a third party pursues a legitimate interest, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Informed consent is, as stated, pivotal to privacy protection. After all, if we as data subjects have given our consent to a website, an app provider, Google, Facebook, Marktplaats, etc., our informed consent is almost a general permit for these organizations that have acquired our informed consent to do whatever they like,

with handling, selling re-selling, allowing usage and/or making profiles (based on) of our data.

April 10, 2018: Senator Lindsey Graham asked Mark Zuckerberg
'You'd embrace regulation?
ZUCKERBERG: The question is, as the internet becomes more important in people's lives, what is the right regulation, not whether there should be or not.
GRAHAM: You, as a company, welcome regulation?
ZUCKERBERG: If it's right, yes.
GRAHAM: Do you think the Europeans have it right?
ZUCKERBERG: They get things right'.

Obviously, the EU did not get things right: less than ten days later Facebook moved 1.5 bn users to the US.[37]

Article 4(11) of the GDPR defines consent as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* Article 29 Data Protection Working Party (Art. 29 WP)[38] released Guideline WP259 on Consent under the GDPR, and stated concerning consent: *'Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment'*.[39]

April 11, 2018: Senator John Neely Kennedy of Louisiana came in peace, so he said, but his remarks were expressed in strong language:
"Mr. Zuckerberg, I come in peace. I don't want to vote to have to regulate Facebook, but by God I will," Sen. Kennedy began his short exchange. "In fact, a lot of that depends on you. I'm a little disappointed in this hearing today, I just don't feel like we're connecting."
He was also quite upset with the way in which Facebook communicated its user data policies to its users. "Your user agreement sucks," he went on. "The purpose of that user agreement is to cover Facebook's rear end, it's not to inform your users about their rights. Now you know that, and I know that. I'm going to suggest to you that you go back home and rewrite it."

EU users have to agree to the same USA originating user policies. So, I am asking you: 'Are we indeed giving our consent in a free, specific, informed and unambiguous manner when we click OK on a question asked by a service provider'? If you, as my audience, apply this test to your own behavior over the last five years when clicking OK to an app-provider and/or service provider, would you then conclude that your consent was informed? I would argue it was not! Let us assume that when your consent was indeed informed: Were you as data subject offered control and genuine choice in accepting or declining? Again, I would argue you were not in control and did not have the feeling of a genuine choice.[40] Reading the EU law as it became applicable on May 25, 2018, this means that no lawful processing of our personal data can be done, due to the lack of a *freely given, specific, informed and unambiguous indication of your and my wishes.*

Some observations

From a legal perspective GDPR defines the requirements so that we give our informed consent. Practically speaking it will not work, so we will keep giving our OK without really knowing to what we consent. Here standardization could be helpful, whereby engineers and lawyers working together on devising a standard to ask questions of a user so that after answering them, real and genuine consent has been given.[41]

Also, a tool developed by consumer organizations or under data protectionist control could help: a little program, available in our browser, that 'carries' or contains our individual wishes concerning the amount of data we want to share when visiting a certain website or using a service.[42]

Artificial Intelligence

Artificial Intelligence (AI) is a transversal technology. It is used in remote controls for TV's and lighting, can be found in smart meters, is important for use in automotive welding robots as well as the driving force behind autonomous cars. AI is vitally important for the application of building secure systems, of our ability to search the internet, driving the use of Big Data, etc. AI is important when used in the physical environment as in welding robots or as a vacuum cleaner in the house.

Even more important and pervasive and invisible is the use of AI in non-physical systems such as software systems, search engines, behavior pattern recognition as well as facial recognition or to sift through immense quantities of data in the search for patterns to diagnose diseases, for example. A subset of software systems is the use of AI in profiling people.[43] And I will focus on this in the coming paragraphs.

Automated decision-making & profiling

Art. 29 WP defined automated decision-making as: *"the ability to make decisions by technological means without human involvement."* These decisions can be based on any type of data, as provided directly by the individual concerned (such as responses to a questionnaire); or data observed about the individual (such as location data collected via an application); and it also can be derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).[44] Automated decisions can be made with or without profiling. Of course, profiling can take place without making automated decisions. But typically, data will be collected to 'construct' a profile that later on will almost certainly be used in an automated decision.

Advertising has always been about demographics and profiles. In information science engineers will nowadays construct and apply user profiles generated through computerized data analysis. This data analysis will be done through AI algorithms or other mathematical techniques, allowing for the discovery of patterns or correlations in large quantities of data.[45] The amount of data that each individual generates every day again and again, mainly through the use of a mobile phone,[46] is immense and has proven to be increasingly valuable to an ever-diminishing group of companies. And this richness has come mainly from using AI techniques in collecting/interpreting individual behavioral data applied to advertising.

Intermezzo
Congresswoman Mrs Eshoo asked Marc Zuckerberg during the hearing on April 12, 2018: "Are you willing to change your business model in the interest of protecting individual privacy?" she asked. "Congresswoman, we have made and are continuing to make changes to reduce the amount of data…" Zuckerberg said. Eshoo stopped him and repeated her question word for word. "Congresswoman, I'm not sure what that means," Zuckerberg said.

The current technology underlying internet and smartphones has now made immediate and personalized advertising possible: 'Advertisers can now post advertising messages, direct to a specific, target audience at the exact moment required'.[47] Only a few years ago this targeting was only precise enough for group

targeting. But AI technology is already closing in on individuals; it is called micro targeting.[48]

GDPR

Article 22[1] GDPR on automatic decision making: '"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." You and I have the right not to be subject to a decision based solely on automated profiling in the event that legal effects or similarly significant effects concerning you or I are produced. This automated decision-making is only allowed if the decision is:

1. necessary for entering into or the performance of a contract between an organization and the individual;
2. authorized by law (for example, for the purposes of fraud or tax evasion); or
3. based on the individual's explicit consent.

Under 3 the word consent is back again, now not as *informed consent* but as *explicit consent*. Scholars and/or privacy advocates have to decide what is meant here. Art. 29 WP has already made an interpretation available:

The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.[49]

Nevertheless, the same comment I voiced earlier on informed consent is applicable here: there is need for a technological, preferably standardized solution so that GDPR indeed leads to more privacy protection.

Micro targeting is (stealthy/secretively) influencing individual choices and is, in my view, captured by article 22[1] GDPR. It is a type of automated processing aimed at legally or similarly significantly affecting the individual, i.e. you buy a product or (do not) vote for a certain candidate in elections.

Conclusion

Hopefully my lecture allows for the recognition that engineers and legally trained people need to work together to regain the terrain lost by the citizens of the world to private firms and authoritarian states. These states are stealthily hijacking one of the most important global standardization organs, the Specialized Agency of the UN: The International Telecommunications Union. This cooperation between engineers and lawyers is even more necessary to safeguard the freedom that was brought by the evolution of the internet and the smartphone. *Laissez faire* is not an option, more dedicated effort is necessary to reconquering the lost terrain.

The big firms evade taxes,[50] evade human rights protection,[51] use psychological insights to make us addicted smartphone users.[52] If these firms want to operate in the EU they need to abide to the law, notably human rights law. I want to close my lecture of today by looking back at the tests I provided in my inaugural address in 1993.

The first test I then provided was to prevent privacy (human rights) infringement by engineering a solution in such a way that no (extra) regulation is necessary. In other words, develop technical solutions that do not need regulatory intervention, make innovative technology human rights-proof. In the context of privacy, GDPR refers to it as: Privacy-by-Design.

The second test I provided was to use human rights as a means or as a requirement for setting certain limits to technological developments: e.g. as in Genetically Modified Organisms where limits have been proposed to only allow these inn the market or in a field, based upon food safety standards.[53]

If we do not act, a lot of internet and ICT based types of technologies, mostly presented to us as a technological innovation, will replace law in crucial areas and the loss of jurisdiction and human dignity will be inevitable.

Notes

1 J.M. Smits, Normalisatie: Recht òf Techniek? Eindhoven, June 11, 1993. I could, with some minor adjustments give the same lecture, and the same questions can still be raised. The same research challenges can still be posed. The same basic framework I suggested then is still applicable. So I would be honored if you read that lecture in conjunction with this one. The text (in Dutch) is available here https://www.researchgate.net/publication/254799919_Normalisatie_recht_of_techniek

2 There are many resources available on the internet and studies on qualifying and explaining different standardization organizations. See Dr. Peter Hatto, Standards and Standardization A practical guide for researchers, EUROPEAN COMMISSION DIRECTORATE-GENERAL FOR RESEARCH & INNOVATION, Directorate G - Industrial technologies, Brussels https://ec.europa.eu/research/industrial_technologies/pdf/practical-standardisation-guide-for-researchers_en.pdf, retrieved April 26, 2018. See also Andrew Updegrove, The Essential Guide to Standards, https://www.consortiuminfo.org/essentialguide/whatisansso.php. An extensive account on the role of standardization, see Standardization in Companies and Markets - Wilfried Hesser (et.al.), available on line: www.pro-norm.de and www.asia-link-standardisation.de, consulted April 26, 2018.

3 Bekkers, R.N.A. (2001). The development of European mobile telecommunications standards: an assessment of the success of GSM, TETRA, ERMES and UMTS. Eindhoven: Technische Universiteit Eindhoven. ((Co-)promot.: Jan Smits & A. Préchal). https://research.tue.nl/en/publications/the-development-of-european-mobile-telecommunications-standards-a.

4 Lim, A.S. (2006). Power battles in ICT standards-setting process: lessons from mobile payments. Eindhoven: Technische Universiteit Eindhoven. ((Co-)promot.: Jan Smits & Geert Duijsters).

5 ITU-T Study Group 2 (SG-2) plays an important role, dealing with naming, numbering, addressing and identification for telecommunications networks (numbering issues). In particular SG-2 manages international telecommunication country codes – E.164 numbers and E.212 international mobile shared codes and a number of other network identifiers. For more information please visit https://www.itu.int/en/ITU-T/about/groups/Pages/sg02.aspx. Uniform Resource Locators (URL's) were defined in RFC 1738 in 1994 by Sir Tim Berners-Lee, the inventor of the World Wide Web. The Uniform Resource Identifier (URI) was defined by the working group of the Internet Engineering Task Force (IETF), RFC 3986 (2005), see for the text https://www.ietf.org/rfc/rfc3986.txt (retrieved April 26, 2018).

6 For an account on how this can be perceived see: The European Union and the GAFA issue, http://eyes-on-europe.eu/the-european-union-and-the-gafa-issue/ consulted April 26, 2018.

7 Submarine and satellite systems regulation was the subject of my PhD: Jan M. Smits, Legal aspects of implementing international telecommunication links: institutions, regulations and instruments: Martinus Nijhoff Publishers, Dordrecht, Boston, London, 1991, 240 pp.

8 For Google, see http://www.datacenterknowledge.com/google-alphabet/three-new-submarine-cables-link-google-cloud-data-centers. For Microsoft and Facebook, see https://thenextweb.com/facebook/2017/09/22/microsoft-and-facebook-just-laid-a-160tbps-undersea-cable-17000-feet-deep/ (consulted April 11, 2018).

9 As an example of how proprietary standards work, and affecting many others: 'App developers won't be able to use Google to get around internet censorship anymore. The Google App Engine is discontinuing a practice called domain-fronting, which let services use Google's network to get around state-level internet blocks. On April 13, 2018 it was gone. A recent change in Google's network

architecture means the trick no longer works. First spotted by Tor developers on April 13th, the change has been rolling out across Google services and threatens to disrupt services for a number of anti-censorship tools, including Signal, GreatFire.org and Psiphon's VPN services.' See https://www.theverge.com/2018/4/18/17253784/google-domain-fronting-discontinued-signal-tor-vpn, retrieved April 26, 2018.

10 Serge J.H. Gijrath (2006), Interconnection Regulation and Contract Law, diss. Tilburg, Promot.: Cees Stuurman & Jan Smits).

11 See for a description of the reason for developing Content Delivery Networks, http://www.etsi.org/images/files/ETSIClusterBrochures/clusters-content-delivery-Q32015.pdf retrieved April 4, 2018.

12 "How content delivery networks (CDNs) work". *NCZOnline*. See https://www.nczonline.net/blog/2011/11/29/how-content-delivery-networks-cdns-work/,'Requests for content are typically algorithmically directed to nodes that are optimal in some way. When optimizing for performance, locations that are best for serving content to the user may be chosen. This may be measured by choosing locations that are the fewest hops, the least number of network seconds away from the requesting client, or the highest availability in terms of server performance (both current and historical), so as to optimize delivery across local networks. When optimizing for cost, locations that are least expensive may be chosen instead. In an optimal scenario, these two goals tend to align, as edge servers that are close to the end-user at the edge of the network may have an advantage in performance or cost.' Retrieved 2 April 2018.

13 Conform http://www.etsi.org/technologies-clusters/clusters/content-delivery, consulted April 4, 2018.

14 For a short summary of the DOA system see https://www.internetsociety.org/resources/doc/2016/overview-of-the-digital-object-architecture-doa, consulted April 21, 2018.

15 For the reasons underlying DOA, see interview with Dr Robert Kahn, co-inventor of the Internet, ITU News nr 4, May 2010, pp 17-21.

16 For a critical account see Robert M. McDowell & Gordon M. Goldstein (Hudson Institute), The Authoritarian Internet Power Grab, WSJ, Oct 16, 2016, https://www.hudson.org/research/12951-the-authoritarian-internet-power-grab, consulted April 11, 2018.

17 See ITU Proceedings of the World Telecommunication Standardization Assembly, held in Hammamet, Tunisia, October 25- November 3, 2016. See http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.311.43.en.100.pdf, retrieved April 27, 2018.

18 The text in this box is the summary in the X.1255 document. The document is available at https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1255-201309-I!!PDF-E&type=items, retrieved April 27, 2018.

19 Anthony Rutkowski, Selling DONA as snake oil at ITU, http://www.circleid.com/posts/20161025_selling_dona_snake_oil_at_the_itu/ consulted April 26, 2018.

20 ISOC, in a blog called ITU WTSA 2016 Outcomes: An Internet Society Perspective, https://staging.internetsociety.org/resources/doc/2016/itu-wtsa-2016-outcomes-an-internet-society-perspective/, made the following remarks: 'Agreement was reached to either replace DOA references with Recommendation ITU-T X.1255 (which is based on the DOA) or remove them entirely from the relevant resolutions if agreed text on identity management would be reflected in the summary record of the proceedings. The compromise text was as follows: "*the Plenary recognized that identity management plays an important role in many telecommunications/ICT services and that it can be implemented using a range of technologies and solutions*." We should expect prolonged debates as DOA has survived with a variety of hooks in Resolutions and Recommendations that will carry into Plenipotentiary 2018. It will be important for governments to consider interoperability, stability,

security and scalability (at Internet scale) capabilities of any technologies that are deployed on the Internet to ensure that the Internet continues to remain secure and stable.' Consulted April 26, 2018.

21 RESOLUTION PLEN/3 (DUBAI, 2012), Dubai 2012, see https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf consulted April 21, 2018.

22 See https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en consulted April 4, 2018.

23 Albeit, this might also be done by the US government: see the plans that oblige you to hand over your email(address), and social media account to be allowed to enter the USA, see proposed changes to ESTA and D160 forms. Already law: the CLOUD Act adds a new section in the so-called Stored Communications Act (SCA), namely 18 USC § 2713, entitled "*required retention and disclosure of information and records.*" This new section stipulates that it doesn't matter where the relevant data sets are located: *"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States*." For comments see: The CLOUD Act — A needed fix for U.S. and foreign law enforcement or threat to civil liberties? https://iapp.org/news/a/the-cloud-act-a-needed-fix-for-u-s-and-foreign-law-enforcement-or-threat-to-civil-liberties/, or see Axel Spies, Louis Rothberg, Congress Approves Data Access Outside of the United States (CLOUD Act) – But the EU May Not Like It, https://www.aicgs.org/about-aicgs/ retrieved April 27, 2018.

24 Fischer, J.C. (2010). Communications network traffic data : technical and legal aspects. Eindhoven: Technische Universiteit Eindhoven. ((Co-) promot.: Jan Smits & N.A.N.M. Eijk, van), https://research.tue.nl/en/publications/communications-network-traffic-data-technical-and-legal-aspects

25 BGH, Urteil vom 25.5.1954, ZR 211/53, NJW 1954, 1401 (Leserbrief).

26 According to E.C. (Eva) Heeger, Controlling your online profile: reality or an illusion? A study of informed consent as a mechanism to regulate commercial profiling, Thesis Utrecht University, School of Law, August 2015, p. 6.

27 ECJ 14 October 2004, Omega Spielhallen--- und Automatenaufstellungs GmbH v. Oberbürgermeisterin der Bundesstadt Bonn (C---36/02). Omega wished, as a service provider from a firm in the United Kingdom, to open a game hall in which individuals could use laser guns to simulate homicide. The ECJ ruled that the German prohibition of this service, which was based upon human dignity, was justified, even though no similar restrictions existed in the United Kingdom.

28 Ibid. nt 26, p. 7.

29 Koops, B.J. (1999). The crypto controversy: a key conflict in the information society. Eindhoven: ECIS. ((Co-)promot.: M.S. Groenhuijsen, Jan Smits & Henk van Tilborg).

30 Bert-Jaap Koops, et. al., A Typology of Privacy, in U. Pa. J. Int'l L. [Vol. 38:2, 2017] pp. 483-575.

31 We need dataspherists, i.e. scientists trained in more disciplines, such as programming, app design, information security, law, ethics and data science.

32 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 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 119/1-88, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=NL retrieved April 26, 2018.

33 Consent is given by an individual here in the context of using services from an internet service provider that, of course, has mirrored rights and obligations. This lecture is too short to also deal with their role in obtaining the individual's consent, and the obligation to be able to prove that consent.

[34] See being a 'Dopamine Machine' on Facebook https://www.quora.com/Is-Facebook-a-dopamine-machine. Ot van Dallen, De zeven privacytrends van 2017, in Mediaforum, 2018-1, p. 2-5, and his references in notes 44, 45, 46 and 47, see also hereunder notes 40 and 52.

[35] By way of example: the TU/e being my employer is the controller in the jargon of GDPR, the firm it requests to process the salaries of all TU/e employees is called the processor and I am the data subject.

[36] Ibid. nt 26.

[37] Facebook, just a few days after the congressional hearing after the Cambridge Analytica scandal, The Guardian, April 19, 2018, Facebook moves 1.5bn users out of reach of new European privacy law (Company moves responsibility for users from Ireland to the US where privacy laws are less strict) https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law , retrieved April 26, 2018.

[38] Article 29 Data Protection Working Party is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission Privacy professionals work in EU in the so/called art 29 WP. http://ec.europa.eu/justice/article-29/documentation/index_en.htm

[39] http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360, Guidelines on Consent under Regulation 2016/679 (wp259) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239 on p. 4. The Guidelines were adopted but not finalized, when consulted on April 28, 2018.

[40] If we add this to the way in which psychology is being used to lure us first into the service provision and second to keep/make us addicted. Sean Parker, Facebook president in an earlier life, said in an interview with the Guardian in November 2017 that Facebook is made in such a way that it exploits human vulnerability. Google, Twitter and Facebook workers who helped make technology so addictive are disconnecting themselves from the internet, they did so because they worked on highjacking our minds, see https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia, April 2, 2018

[41] In 2017 a tool, an automated decision tree based upon the requirements of the GDPR concerning informed consent, was developed under my supervision by two Bachelor students (Zoetbrood & Mohan) as an assignment for Fourtress. If you want to find out what questions should be asked to genuinely ask for your consent and/or what data can be collected lawfully by a company or organization, go to www.gdpr-informedconsent.eu, to check for yourself. Depending on the answers either a user perspective or an organization perspective is supported.

[42] Ghostery, see https://www.ghostery.com/, but also privacy badger by Electronic Frontier Foundation https://www.eff.org/nl/privacybadger, or duckduckgo.com provide already some protection from being tracked all over the internet.

[43] Nuria Oliver on AI: https://www.euractiv.com/section/digital/video/game-changers-nuria-oliver-on-artificial-intelligence/

[44] Article 29 Data Protection Working Party: Website: http://ec.europa.eu/justice/data-protection/index_en.htm WP 251 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018.

[45] Read the warnings concerning the value of these AI algorithms in Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown Publishing Group/Penguin Random House, New York 2016. Check her blog out regularly on mathbabe.org.

[46] And it will grow exponentially after the full rollout of IoT devices, by 2025 the installed base of IoT devices will be over 75.4bn devices, see for example: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#1461fd821480, consulted April 28, 2018.

47 Multiple sources: https://www.linkedin.com/pulse/profiling-real-time-bidding-take-online-advertising-up-namon-kent

48 I will leave the psychological and neuro science ways of influencing/nudging people aside here, but as early as 2008 questions were raised whether Facebook was a dopamine machine, e.g. see Susan Weinschenk's book Neuro Web Design: What Makes Them Click? (Voices that matter), Berkeley, CA 2008. Even earlier, in 1984, Sherry Turkle wrote at a more abstract level in The Second Self about how computers are not tools as much as they are a part of our social and psychological lives. In 1995 Life on the Screen followed in which she discusses how emerging computer technology affects the way we think and see ourselves as humans.

49 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679 Adopted on 28 November 2017, WP259, Brussels 2017, p. 18.

50 See https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en Consulted April 4, 2018.

51 Facebook, just a few days after the congressional hearing after the Cambridge Analytica scandal, The Guardian, April 19, 2018, Facebook moves 1.5bn users out of reach of new European privacy law (Company moves responsibility for users from Ireland to the US where privacy laws are less strict) https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law, retrieved April 26, 2018.

52 Ibid nt 34, on Addiction, Jessica McGreal, Smartphone addiction in 5 charts, see https://www.raconteur.net/technology/smartphone-addiction-in-5-charts , April 4, 2017. Retrieved April 26, 2018.

53 Here it is about authorizing the market availability of food that has been technologically changed: genetically modified organisms. The limitation requirements are not human rights but food safety. In the wording of the European Food Safety Authority: 'Genetically Modified Organisms (GMOs) are organisms whose genetic characteristics are artificially modified in order to give them a new property. They can, for example, be plants or crops that are resistant to drought, tolerant to herbicides or to certain insects or that have an improved nutritional value. The placing on the market of GMOs in the EU is strictly controlled. GMOs can only be used in the EU if they are authorized beforehand. And they are only authorized once they are deemed safe for humans, animals and the environment. Once authorized, they have to be adequately monitored for any unforeseen effects.' The EU explained: Agriculture, Food safety from farm to fork: safe and healthy food for everyone, Brussels 2014, p. 12, See (retrieved April 2018).

Curriculum Vitae

Prof. Jan Smits has been professor of Law and Technology at the Department of Philosophy and Social Sciences since 1992, later at the subdepartment of Innovation Sciences at Eindhoven University of Technology.

Prof. Jan Smits studied law in Tilburg, worked at Universities of Nijmegen and Utrecht, where he defended his PhD in 1990. His research in the first fifteen years of his appointment mainly focussed on (mobile) telecommunication and digital tv. The last decade on privacy protection and information security. He found that non-technical disciplines have a difficult time at a technical university, because they are not core disciplines for an engineer. However, it is precisely the humanities and social sciences can provide colour and richness to the engineering programs. From this point of departure, Prof. Smits has always given his education with great pleasure and passion.

His social commitment took shape in the Brainport region: municipalities Heeze-Leende, Waalre and recently Helmond, decided to build fibre optic networks for all its citizens, thanks to his opinionated view regarding European law and from his unshakable conviction that what is common needs to be public. He co-founded Brainport Center for Technology and Law in order to let engineers see that where the law is often perceived as an obstacle, it is also possible to see it as a design tool.

Colophon

Production
Communicatie Expertise Centrum TU/e

Cover photography
Rob Stork, Eindhoven

Design
Grefo Prepress, Eindhoven

Print
Drukkerij Snep, Eindhoven

ISBN 978-90-386-4541-4
NUR 950

Digital version:
www.tue.nl/lectures/

Visiting address
Auditorium (gebouw 1)
Groene Loper, Eindhoven
The Netherlands

Navigation address
De Zaale, Eindhoven

Postal address
P.O.Box 513
5600 MB Eindhoven
The Netherlands

Tel. +31 40 247 91 11
www.tue.nl/map

Technische Universiteit
Eindhoven
University of Technology