VU Research Portal

Data Algorithms and Privacy in Surveillance

Lodder, Arno R.; Loui, R.P.

published in

Research handbook on the law of artificial intelligence
2018

DOI (link to publisher)

[10.4337/9781786439055.00025](https://doi.org/10.4337/9781786439055.00025)

document version

Publisher's PDF, also known as Version of record

document license

Article 25fa Dutch Copyright Act

[Link to publication in VU Research Portal](#)

citation for published version (APA)

Lodder, A. R., & Loui, R. P. (2018). Data Algorithms and Privacy in Surveillance: On Stages, Numbers and the Human Factor. In W. Barfield, & U. Pagello (Eds.), *Research handbook on the law of artificial intelligence* (pp. 275-284). Edward Elgar. <https://doi.org/10.4337/9781786439055.00025>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

13. Data algorithms and privacy in surveillance: on stages, numbers and the human factor

Arno R. Lodder and Ronald P. Loui

I. INTRODUCTION

Surveillance opportunities are almost limitless with omnipresent cameras, constant internet use, and a wide variety of Internet of Things objects.¹ We access the Internet anytime, anywhere via smart devices such as phones and tablets, and gradually more objects become connected. In the Internet of Things not only computing devices but all kinds of ordinary objects are provided with an IP address such as books, food, clothes, cars, etc.² All our online interactions generate a stream of data. On top of data generated by ordinary internet use comes the use of wearables, smart meters, connected cars and other features. The process of almost unlimited data generation is labeled as datification.³

Humans can process only small amounts of data, computers can process almost infinitely. But also computers need to act smart or intelligent, because otherwise even they get swamped and/or might produce useless information. Algorithms help in structuring and analyzing vast amounts of data. With the growth of data we have to rely increasingly on algorithms. These algorithms may perform better than alternative approaches we used to rely on.⁴ However, algorithms can be opaque, and the danger is that we get obscured by algorithms.⁵

In the wake of the Snowden revelations awareness in society has grown about what digital technologies offer in terms of surveillance and control.⁶ The scale of mass surveillance by governments around the world through, for example, the bulk collection of metadata⁷ and the monitoring of social media shocked even the most well informed individuals. Data mining and surveillance within the law enforcement and national security contexts

¹ T. Wisman, *Purpose and Function Creep by Design: Transforming the Face of Surveillance through the Internet of Things*. European Journal of Law and Technology (2013) Vol. 4, No. 2.

² A.D. Thierer (2015), *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*. Rich. J. L. & Tech. (2015) 21, 6.

³ S. Newell and M. Marabelli, *Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of 'Datification'*, Journal of Strategic Information Systems (2015) 24(1).

⁴ Anupam Chander, *The Racist Algorithm?* 115 Mich. L. Rev. 1023 (2017).

⁵ F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

⁶ B.C. Newell, *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe*, I/S: A Journal of Law and Policy for the Information Society (2014) Vol. 10(2), 481–522.

⁷ J.C. Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs* ISJLP (2014) 10 301.

raise serious human right rights concerns⁸ about the ability of modern states to monitor, oppress and control their citizens.⁹

Not all algorithmic outcomes are adequate.¹⁰ For instance, recently mortgage providers complained about the fact that algorithms advised in too many cases against a mortgage, also if it was quite obvious the person who requested was reliable and creditworthy. For instance, it is known that musical preference matters. If one law professor likes Bach and Mozart, and the other hip hop (e.g., derived from Facebook preferences), the algorithm might decide that the latter is not getting the mortgage.

Here is where the human factors issues enter. A human could easily decide against the algorithm, viz. that a tenured law professor with a preference for hip hop music is creditworthy. What the example also illustrates is that data processing algorithms can seriously impact our private lives.

Intelligence agencies use algorithms to distinguish between persons of interest and others. Law enforcement uses analytics and data mining to identify suspects and to support investigations. Businesses profile users in all kind of categories. Surveillance is omnipresent. The impact on privacy is not necessarily depending on who does the surveillance. It depends not only on the actors, but on various factors. Sometimes what businesses do impacts severely on the privacy of consumers, sometimes the work of police or intelligence agencies does not. In this paper we focus on surveillance by the US National Security Agency (NSA) and other intelligence agencies. Our aim is to dissect data analytics by intelligence agencies, and to suggest what privacy related law should focus on more than it does today.

With an understanding of how big data algorithms usually work we discuss in this chapter the use of algorithms from a privacy and data protection angle. First, we briefly introduce the central concepts of data protection and privacy against the background of the General Data Protection Regulation¹¹ introduced by the European Union in 2012, published in 2016 and effective as of 25 May 2018. The core of the chapter consists of elaborating upon three issues:

1. The stages of data processing while using algorithms, how it affects privacy and what safeguards the law should provide;
2. The role of the human factor: how and when should humans be involved in evaluating outcomes, and also under what circumstances human interference is better abstained from;
3. The relevance of scale and scope: in the light of privacy, numbers matter. However, so far in law a discussion on the relevance of numbers (or scale) is largely absent.

⁸ A.D. Murray, *Comparing Surveillance Powers: UK, US, and France* LSE Law Policy Briefing Papers: SPECIAL ISSUE: The Investigatory Powers Bill (14/2015).

⁹ L. Colonna, *Legal Implications of Data Mining. Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices*, Ph.D thesis Stockholm, 2016.

¹⁰ L. Rainie and J. Anderson, *Code-Dependent: Pros and Cons of the Algorithm Age*, Pew Research Center, February 2017.

¹¹ 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), *Official Journal L 119*, 4/5/2016, pp. 1–88.

II. PRIVACY AND DATA PROTECTION

Goldsmith and Wu¹² considered the European Union Directive 95/46¹³ on data protection controversial due to its aggressive geographic scope. Article 4(1) of that Directive states that besides data controllers established in the EU, the Directive applies to controllers outside the EU if by virtue of international public law one of the EU member states' law applies or in case equipment is used that is physically located in an EU member state. The territorial scope of Article 3(2) GDPR is way more aggressive. The regulation applies to:

the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

So, the GDPR applies to all internet services delivered to EU citizens: indifferent where the service provider is located, be it the USA, China, Brazil, Nigeria, etc. Stating to have jurisdiction is obviously not the same as being able to enforce the law, but companies who trade with EU citizens probably see no other option than to comply.

The rules in the GDPR are centered basically around the principles (listed in Article 5(1)) already described in the OECD principles of 23 September 1980 on governing the protection of privacy and transborder flows of personal data, such as purpose limitation, data minimisation, and accuracy. New is the explicit accountability duty for the controller in Article 5(2): "The controller shall be responsible for, and be able to demonstrate compliance with. . .". Other novelties are i.a. explicit mentioning of data protection by design and data protection by default (Article 25), the obligation to keep records of processing activities (Article 30), Data Protection Impact Assessments (Article 35), and a formal, central role for the Data Protection Officer (Articles 37–39).

In particular of relevance for this chapter are the rules on profiling, defined in Article 4(4) as:

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. . .

Although by nature big data and profiles form a risk for infringements of privacy and data protection, in particular in our present day data economy (cf. datafication), the GDPR addresses the topic of profiles.¹⁴ Article 21(1) states that the data subject

¹² J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006) p. 175.

¹³ 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, *Official Journal L 281, 23/11/1995*, pp. 31–50.

¹⁴ D. Kamarinou, C. Millard and J. Singh (2016), *Machine Learning with Personal Data* Queen Mary School of Law Legal Studies Research Paper No. 247/2016.

has a right to object to profiling “on grounds relating to his or her particular situation, at any time”. There is, however, a way out for the data controller, since he can continue with the processing in case there are “compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.” One can imagine the data controller is relatively easily convinced by its own grounds, rather than the interests of the data subject. The other right is in Article 22(1) to “not 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.” This Article expresses the fear to trust the machine, and could already be found in Article 15(1) of the Directive 95/46:

grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Our focus here is on “the processing” and the “decision based solely on automated processing.” The idea that all stages in the processing are subject to the same calculus of potential override is flawed. The idea that automated decisions always put the individual at greater risk for encroachment on rights also needs more nuance.

For the police the rules on profiling are slightly different, and not based on the GDPR but a separate EU Directive for police and justice.¹⁵ It prohibits profiling “which produces an adverse legal effect concerning the data subject or significantly affects him or her . . . unless authorised by law . . . and which provides appropriate safeguards for the rights and freedoms of the data subject” (Article 11(1)). Special for the area of police and justice is the rule on profiling that results in discrimination, which is always prohibited (Article 11(3)).

Without further going into details of data protection regulations in relation to big data¹⁶ it is clear that not all relevant aspects of big data analytics and the use of algorithms are addressed. The remainder of this chapter discusses some aspects that are often overlooked in this context but we believe need to be taken into account when thinking about the use of algorithms and the possible impacts on data protection and privacy.

¹⁵ DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *Official Journal L 119*, 4/5/2016, pp. 89–131.

¹⁶ B. van der Sloot, *Privacy As Virtue: Moving Beyond the Individual in the Age of Big Data*, Ph.D Thesis University of Amsterdam, 2017.

III. STAGES IN THE ALGORITHM

The huge controversial fallout over Edward Snowden's disclosures and NSA surveillance programs¹⁷ shows that Judge Posner was right:¹⁸ there are privacy encroachments that have huge consequences and there are privacy encroachments that have almost no consequences. It is important for legislation to distinguish the two. But how?

The legislation must refer to the algorithm, or at least the stages in the algorithmic process.¹⁹ The public focus is traditionally on initial collection of data. Collection is the starting point of processing, and sets the stage for eventual legitimate further processing. What the law does not take into account, is that stages differ in their privacy risks and implications. At some stages, there may be many persons susceptible to small risks. Those risks may mainly be the exposure to the possibility of further consideration at a later stage. At a later stage in the algorithm, the risks to an individual's privacy, and more, may be great, but the numbers at risk at that stage may be small.

The NSA and The United States Foreign Intelligence Surveillance Court (FISC) regulated the process of programmatic warrants that specified the bulk collection. Separately, it regulated the individualized warrants for individuals used as selection terms for searches of databases. But both were guilty of not disclosing the important winnowing of the numbers during processing: collection (logging and warehousing), followed by n-hop discovery in social network analysis, followed by deletion of most records, followed by entry into the "corporate store", where a record was susceptible to search by an analyst. These are at least five stages of algorithmic processing.

At each stage, an individual was exposed to a different risk. At each stage, a different degree of automation and comprehension was employed. And at each stage, a different number of individuals were exposed. In fact, the rate of reduction from stage to stage was staggering: for every 100 million call detail records retained, the NSA discarded trillions, or tens of trillions, for a 1000:1 or 10000:1 rate of reduction.

Surely it is the obligation of effective regulation to refer to each stage of the algorithm separately, as the implications for privacy are so different at each stage.

A. The Same Algorithm with Different Numbers and Risks

The source of controversy surrounding the NSA, and intelligence agencies in general, partly is caused by an inadequate interpretation of the different numbers and risks. The actual process, with mainly algorithmic risk at stages where large numbers were involved, was not much to complain about. But the same process, with a different set of risk exposures at each stage, could be a clear violation of privacy protections, truly analogous to a digital secret police state activity. FISC should have specified not just the

¹⁷ N.A. Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*. *ISJLP* (2014) 10: 523.

¹⁸ R.A. Posner, *Privacy, surveillance, and law*. The University of Chicago Law Review (2008) 75, no. 1: 245–60.

¹⁹ K. Yeung, *Algorithmic Regulation: A Critical Interrogation*. Regulation and Governance (2017).

warrant-granting process, but also placed explicit limits on the practical effects at each stage, especially the numbers of persons at risk of further analytics.

Would it make a difference if a human were engaged at every step, or at only the final step (which in fact was the case in the NSA Social Network Analysis)? Would it make a difference if the final step produced no more than ten persons, say, as a limit to human analyst search of the corporate store? Or if no more than 1000 new individuals' data, per year, entered the corporate store for persistent availability longer than six months? What if the risk of being reviewed by automated methods at the first stage were reduced, so that randomly, one percent that could be connected under Social Network Analysis were actually retained for the next stage of processing? Would that not change the pragmatic risk of being under surveillance, at that stage? Or suppose that anyone not connected in the current month, under Social Network Analysis, could not be susceptible to retention through a Social Network Analysis connection in the immediate subsequent month? Surely that would reduce the pragmatic risk of surveillance at that algorithmic stage.

Astronomical numbers leave at first sight the impression that the privacy of many is violated during the first stages. What is necessary to be taken into account is what is exactly happening, and when.

There may yet be social implications of privacy encroachments that are very different from the individual implications; what may not affect more than 1000 individuals at a stage of processing might still be unacceptable with respect to societal norms, safeguards, and aims. For example, even if a mere ten persons were subject to human scrutiny at the final stage of algorithmic processing, if those persons were all minorities and selected based on minority status, there may be different legislative considerations in play.

Focusing on individual risk, however, leads to some interesting clarifications. Not all eyes and ears are the same. Computers are not the same as humans when they look. Most of the time the computer is logging benignly, in a way that lots of other computers in the communications path might be logging. Data collection that is mere logging is clearly less invasive than data collection that directly produces a list of persons of interest. Much of the time, an algorithm is looking at a record in order to discard it as uninteresting. That is in fact why automated methods are used as an automatic front end when processing huge volumes of data.

IV. THE HUMAN FACTOR

A. Not all Human Looking is the Same

There is a difference between looking by the machine and looking by humans. Not even all humans are the same. Some are not paying attention. Their surveillance is different from the surveillance of a probing, paranoid, or aggressively inferential mind. Some humans have more experience, understanding, or simply better hearing and eyesight, memory, and gestalt pattern recognition. Some humans can read lips or interpret body language. Canine surveillance, because of superior and unexpected sensory inputs, is different under the law. Some human surveillance and discovery takes place under warrant; some is inadmissible. Some recordings, audio, video, and photographic, are reviewable by humans. Listening to live audio once is different from listening with more time, filtering,

enhancement, signal-to-noise ratio, dynamic range, and frequency-based equalization. It is remarkable that wiretap laws do not make more of these issues.

Wiretap is not even the right analogy. Computer logging of data is more like video camera surveillance, where the search takes place post hoc, with search terms or search parameters, and a specific sort of thing to be found (e.g., a shared rental agreement or airplane ticket). No doubt, relying on *Smith v. Maryland*²⁰ was convenient for US intelligence agencies to escape Fourth Amendment language in a hurry. But pen registers generate logs that can be comprehended by a human, while internet activity generates logs that must be processed algorithmically. They must be searched with some specificity or direction in order to produce discovery and inference. Of course, analytics on streaming text has in the past been more active than video scenes being sent to VCR or DVR. Smart video, of course, is beginning to resemble text analytics on streams and logs.

Not all humans are the same, further, because some humans carry guns. Others can have people arrested. Even non-human processing, at some stage, might carry the risk of harassment, exclusion from access to air transportation, foreign travel, or freedom of motion. Would it not make a difference if such risks from an automatic classifier applied to all persons at the collection stage, or whether such risks could apply only to persons who passed Social Network Analysis, were entered into the corporate store, were produced under human analyst search that required warranted search terms, after the 10000:1 winnowing?

B. Not All Computers Looking are the Same

What we have learned in the past two decades is that not all automata are the same with respect to subjecting individuals to analytics. What a drone can surveil, what can be gleaned from crowd-sourced data, or repeated study, pixel-by-pixel, of incidental video collection, what can be discovered by classifiers trained to find hidden structure and hidden criteria: these are important aspects of privacy for those who have privacy interests under the law. It is not sufficient to regulate collection or non-collection.

It should matter whether personal data is used in pursuit or profiling of that person, or whether the personal data is just used for determining base rates of what is normal. Many abnormality-detecting algorithms require the modeling of what is the “base rate.” For the individual, this may be as simple as counting how many times the most average person uses the word “the” in the most average text. These machine learning methods look at a person’s data precisely because that person is completely uninteresting.

Different kinds of AI may be relevant too. Logging is the lowest form of looking. But translating, parsing, and extracting topics and sentiments from text, automatically, may be more like a human looking. Face recognition is certainly a higher form of processing, and it can put individuals at higher risk at that stage because the inferences are more specific to the individual.²¹ Biometric methods for access to secure places and accounts are now known to have unintended privacy risks that are potentially severe.²² Scanning the

²⁰ *Smith v. Maryland*, 442 U.S. 735 (1979).

²¹ A.G. Ferguson, *Big Data and Predictive Reasonable Suspicion*. (2015) 163 U. Pa. L. Rev. 327.

²² D. Sherman, *Biometric Technology: The Impact on Privacy*, CLPE Research Paper No., 2005.

retina, pulse, and perspiration, or analysing the voice, can reveal increased probabilities for glaucoma, diabetes, stroke, congenital defect, speech impediment, and so forth.

It is not the complexity of the algorithm or the amount of data, but the risk of inference, intended and unintended. The risk of certain kinds of inferences comes with the potential damage that a person will be classified. Classification leads to denial of rights or worse. These are the things that concerned Posner, and should be considered explicitly by regulations. These are more important than fighting over the two extremes of collect-it-all and collect-none-whatsoever.

More importantly, from a potential consequence point of view, the risk of being profiled by an advertiser is usually considered to be much less than that of being profiled by law enforcement. An unwanted ad is not as bad as an unwanted knock on the door. But the possibility, and high probability, of losing the profile to a malicious third party actually reverses that inequality: usually the kind of data available to an ad agency is of higher quality, greater quantity, and longer time frame, than the data available to the government. Blackmail and identity theft are worse consequences, usually, than an hour long due diligence interview with DHS agents because an electronic connection was made between a known foreign agent and an innocent person.

C. AI is not Human Comprehension

Perhaps the most profound confusion in the public's understanding of the NSA Section 215 activities was the conflation of human comprehension with artificial intelligence "comprehension." The public is becoming more aware about big data and AI in news reporting. It is not surprising, given the way that AI is portrayed, that people fear the privacy incursions of AI the way they would feel if the AI were replaced by a human. But of course, the AI is there because a human was unsuitable: either too slow, too unreliable, too easily bored or tired, too expensive, not facile with foreign language, not trained to optimal discrimination with respect to narrow criteria. AI is a business decision to automate, usually based on the quality of automation. But there is another reason to insert the AI: it has a natural uninterest in aspects of data that might impact an individual's privacy concerns. It doesn't gossip; it can't be distracted by irrelevance; it forgets what it is told to forget; it is not subject to human subterfuge or machination.

AI, analytics, and other algorithmic filtering are not at all like human looking when it comes to privacy. What matters are the potential consequences of the AI decision: the classification, the false positives, and the false negatives. When there is a pipeline of processing, as there was for the NSA, the consequences of classification at one stage are mostly the exposure to further processing at the next stage. This is where legal language that preserves the rights of citizens must bind.

V. ON NUMBERS: RELEVANCE OF SCALE AND SCOPE

What has not yet been learned over the past decades is that numbers matter. An NSA Social Network Analysis program that produced 1,000,000 new names, with data saved in the corporate store for human analytic purposes, for two years at a time, is problematic

no matter how the Social Network Analysis is justified. No doubt, 3-hop Social Network Analysis became 2-hop Social Network Analysis on such numerical considerations.

In the Apple versus FBI fight over unlocking a terrorist's iPhone, numbers mattered.²³ If the FBI were limited to ten, 100, or even 1000 such requests per year, with no serious collateral weakening of Apple's security, that would be acceptable to most citizens. It would balance the relevant interests under the law. There must be a number, however, perhaps a rate of 100,000, or 1,000,000 per year, at which the balance is clearly upset. Regulatory language avoids numerical limits and fractional rate guidelines, but sometimes a number sets forth the desired balance.

Law and computing both tend toward binary distinctions, with error-free discriminators. But practical judgement may simply be about having the right numerical proportions.

A. Privacy Versus Security and Proper Balance of Risk and Exposure

Many think that the fundamental contest in the NSA/Snowden affair was between privacy and security. But these two are not necessarily opposed.²⁴ Increasing perimeter security can have benefits for free and open society within. Increasing privacy, especially against massive data loss and data theft by hackers, can increase security. This is because loss of personal data leads to more phishing and blackmail. Not collecting the data in the first place means no risk of losing the data en masse.

Managing risk is the correct way of looking at the problem. We must keep in mind that there are several different stages in a pipeline of processing, where many are exposed to the first stages, and few to the latter stages, and where earlier stages have few potential consequences, but latter stages may have serious entailments. This is true of many government and legal filtering processes, and it is a particularly appropriate view of analytics on data collected under programmatic warrants.

The question should always be, are there too many persons exposed to too much risk at any stage? It is not effective to argue that 100 million persons were exposed to the risk of future processing, and that future processing culminated in a severe curtailment of liberties. How many persons made it to that last stage? What were the criteria for retention from one stage to the next? If at some point there was deanonymization, so names and identities were available to cross-reference with other databases, was that premature considering the legitimate aims of the process?

VI. CONCLUSION

Algorithms and artificial intelligence can be very powerful, and in the context of surveillance can do things ancient suppressors might have only dreamt of. We have to be cautious in applying the new technologies. Law provides the boundaries of what we should permit

²³ M. Skilton and I. Ng (2016). *What the Apple versus FBI debacle taught us*. Scientific American blog, available at <https://blogs.scientificamerican.com/guest-blog/what-the-apple-versus-fbi-debacle-taught-us/>.

²⁴ D.J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011).

to be done by technology. In this chapter we elaborated on what should be thought of legally when regulating algorithms and privacy in surveillance. The present legal frameworks omit at least three angles.

First, the stages of the algorithmic process should be included in what legal constraints apply to these activities. Collection, selection, deletion, access, etc. are headed under the general concept of processing of data, but should be separately addressed. Second, the law should take into account the difference between people and machines. Some things people do are more infringing than what computers do, and vice versa. Making the right distinctions is needed. Third, the law should think more about numbers. Lawyers do not like it to be that precise, but at least particular margins or bandwidth could be indicated. This also helps in separating different degrees of privacy infringements.

SOURCES

List of Cases

Smith v. Maryland, 442 U.S. 735 (1979).

List of European Legislation

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, Official Journal L 281, 23/11/1995, pp. 31–50.

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), Official Journal L 119, 4/5/2016, pp. 1–88.

DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal L 119, 4/5/2016, pp. 89–131.