DOI 10.5817/MUJLT2015-1-8

THE (UNCERTAIN) FUTURE OF ONLINE DATA PRIVACY[1]

by

DAN JERKER B. SVANTESSON*

In this article I will address a somewhat eclectic selection of data privacy topics that I think are of particular significance, including:

- *Some international developments in the data privacy law area;*
- *Extraterritoriality issues including the 'jurisdictional lasagne';*
- *The recently decided Court of Justice of the European Union (CJEU) case on the so-called 'right to be forgotten';*
- *'Big Data' and the Internet of Things; and*
- *The concept of 'consent'.*

KEY WORDS

Data Privacy, Data Protection, Privacy, Extraterritoriality, Google Spain, Right to be forgotten, Big Data, Internet of Things, Consent

1. THERE IS ACTUALLY A DATA PRIVACY WORLD BEYOND EUROPE...

The reality is that, in the data privacy arena, there is so much going on just in Europe that the task of looking beyond Europe is often unrealistic for Europeans. Yet, I think it is extremely important that Europe does indeed look at what goes on in data privacy in the rest of the world. If that is done, it will not only give a better understanding of relevant foreign law, it may

[1] This article was supported by Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

* Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden).

also make Europe reconsider some of the approaches taken in the proposed Regulation. As noted by Bogdan (2005):

> Foreign law can play an important role for law students … in order to give them a better understanding of their own legal system. … The students begin to see their own legal system from a new point of view and with a certain distance; they realize there is nothing God-given about its rules. For this purpose, substantive foreign law should be taught within the framework of all regular courses, even if only by way of a few well-chosen examples rather than in a consistent and comprehensive way.

This is as true for data privacy European law makers as it is for law students.

European interest in data privacy beyond Europe seems to have been largely limited to what goes on in the US. This may be natural given the degree of transatlantic controversy that has stemmed from the data privacy field. However, Greenleaf (2014, p. 493), who has carried out extensive research into data privacy laws around the globe, has shown that by mid-2014, 103 countries across the world had enacted national data privacy laws. With 50 of those countries being outside Europe, soon there will be more non-European countries with data protection laws than there are European countries with such laws. And in light of this, Greenleaf (2014, p. 493) is of course correct in pointing out that innovation in data privacy law is no longer just coming from Europe.

This is important to remember. Europe has and will have the most advanced data protection law in the world, but that does not mean that all aspects of foreign law are inferior or on a lower level than what we find in Europe. Thus, compliance with EU law does not guarantee compliance with all foreign laws.

Further, for Europe to continue to play a central role in shaping the global balancing between data privacy and competing interests, Europeans will have to take greater steps to familiarise themselves with data privacy developments outside of Europe and the US.

Doing so will also be in the interest of European business. After all, European data privacy law is not alone in its approach to extraterritoriality.

In fact, while exceptions can be found (e.g. current Japanese data privacy law), there is a tendency of data privacy laws around the world to adopt an extraterritorial scope so that European businesses doing business in Australia or Singapore will be bound to abide by Australian and Singaporean data privacy law (Svantesson 2013a).

In this context, it is also worth recalling that some non-European data privacy laws make possible the awarding of heavy penalties. For example, Trinidad and Tobago's Data Protection Act 2011 imposes fines up to 10% of the offending party's annual turnover (s. 69).[2] In light of this, the wisdom of justifying breaches of the law by reference to the obvious enforcement difficulties may be called into question.

2. … BUT DATA PRIVACY LAW IS MISSING IN MANY PARTS OF THE WORLD

So far my focus has been on highlighting that there is also a data privacy landscape outside Europe. Yet, it may be equally important to remind Europeans of how well protected their data privacy is compared to in many other parts of the world. Put in the fewest words, Europeans can be seen to be spoilt when it comes to data privacy protection. While Europe debates the bubbles in its 'privacy champagne', large parts of the world are desperately hoping to get access to 'privacy water'. Perhaps it is the luxury of having such strong data privacy protection that has prompted many academics in Europe to be critical of data privacy as such?

At any rate, all this may be worth remembering when one is debating the proposed data privacy Regulation. I am afraid too many European are too quick to dismiss the whole idea of data protection and calling privacy dead – someone cleverly describing privacy as a zombie (Koops 2014, p. 259): it is dead it just doesn't know it yet. But privacy is a fundamental human right even if it is hard to protect and enforce in today's information society.

3. EXTRATERRITORIALITY – THE MOST IMPORTANT DATA PRIVACY ISSUE

So what provision of the proposed EU data privacy Regulation would a non-EU business be most interested in? Well it is certainly not the

[2] For more information about this Act, see: Edmund D Christo 2013, 'Data Protection in Trinidad and Tobago', International Data Privacy Law, vol. 3, no. 3, pp. 202-9.

requirement of a Data Protection Officer, and it is not even the so-called right to be forgotten that has gained so much attention lately. The provision of the proposed EU data privacy Regulation that is of the most interest for a non-EU business is of course Article 3, which outlines the extent to which the Regulation applies to businesses located outside the EU. Here I will devote some effort to analysing the Regulation's approach to extraterritoriality. But first it is interesting to consider what policy goal the EU is pursuing through the approach it has taken.

In a speech on 4 March 2014, European Commission Vice-President Viviane Reding stated:

> On territorial scope I recall the broad support that was voiced for making sure that non-European companies, when offering services to European consumers, apply the same rules and adhere to the same levels of protection of personal data as European companies. This is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world.

This argument does not lack merit. However, the idea that the Regulation's wide reach creates a 'fair competition in a globalised world' is questionable. In fact, complying with the complex EU data privacy law is likely to be prohibitively expensive for small and medium sized non-EU businesses interacting in the European market on an irregular basis. The result will be that only large foreign businesses, and foreign businesses that do not care about complying with EU law, will be able to afford to enter the European market.

3.1 AN ANALYSIS OF THE PROPOSED ARTICLE 3

Despite being so important, Article 3 – determining the proposed Regulation's territorial scope – has received limited attention.

In the form it was presented by the Commission (Proposal 2012), Article 3 reads as follows:

> Article 3:
> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

> 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
> *(a) the offering of goods or services to such data subjects in the Union; or*
> *(b) the monitoring of their behaviour.*
> 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law. (emphasis added)

Anyone attempting to get clarification as to the exact meaning of this Article, and the underlying principles that has guided the drafters, will logically turn to the Explanatory Memorandum. Unfortunately, doing so is an utter waste of time. Depending on one's personal disposition, one will be either amused, dumbfounded or feel great despair in finding that under the heading '3.4 Detailed explanation of the proposal', all that the Explanatory Memorandum states about Article 3 is that: 'Article 3 determines the territorial scope of the Regulation.' If this is the 'detailed explanation of the proposal', we need the drafters to provide a 'super-extended director's cut' version as well.

This lacking attention to a key provision, that more than any other needs to be discussed in detail, is puzzling. What is worse, even on a charitable interpretation of the situation, the failure to provide reasonable guidance as to Article 3 is negligent, arguably suggesting that inadequate attention has been given to the territorial scope of the Regulation. At worst, it seems the drafters are seeking to avoid attention being directed at the enormously important effect of Article 3.

Interestingly, and no doubt controversially, whichever version of Article 3 is finally entering into force, this provision seems likely to bring all providers of Internet services such as websites, social networking services and app providers under the scope of the EU Regulation as soon as they interact with data subjects residing in the European Union. While this can be said to be the case already under the current EU approach to extraterritoriality, it is submitted that the new approach, as found in the proposed Regulation, goes even further.

In more detail, the rule articulated in Article 3(2)(a) contains a double requirement; that is, (1) the data subject must reside in the European Union (similar to passive nationality), and (2) the conduct must take place in the EU (similar to objective territoriality). However, Article 3(2)(b), which must be read independently from Article 3(2)(a), only contains the first requirement – it only focuses on whether the data subject resides in the European Union.

If this is correct, then Article 3(2)(b) suggests that EU residents enjoy the protection of the Regulation simply by residing in the European Union. In the absence of further restrictions, this protection would then seem to attach to the very person of EU residents so as to enable them to rely on this protection also when traveling outside the EU. For example, an EU resident on holiday in New York would be protected by the EU data protection Regulation by virtue of EU residence if a US controller, not established in the Union, processes personal data of the EU resident as part of monitoring the EU resident's behaviour in New York.

This result is so absurd, and so clearly inappropriate, that it cannot have been the drafters' intention. Thus, the proposed Regulation must be amended to address this issue, and indeed, all that is required to address this particular issue is to include, in Article 3(2)(b), the words 'in the Union' in the manner done in Article 3(2)(a).

Indeed, some experts seem to take such an amendment to Article 3(2)(b) for granted. In expressing his views on the proposed Regulation, the European Data Protection Supervisor (2012, p. 17) stated that:

> [h]e considers that the offering of goods and services or *the monitoring of the behaviour of data subjects in the Union* makes much more sense and is more in line with the reality of global exchanges of information than the existing criterion of the use of equipment in the EU, under Article 4(1)(c) of Directive 95/46/EC. (emphasis added)

While this interpretation is sensible, it would be much more comfortable to have the text of Article 3(2)(b) amended so as to cement this interpretation beyond any doubt.

When the European Parliament had its say on how the Regulation's scope of application is to be delineated, it did indeed address the problem I

pointed to above. The European Parliament's (European Commission 2014, p. 6) version of Article 3 reads as follows:

> Article 3: Territorial Scope
> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether the processing takes place in the Union or not.
> 2. This Regulation applies to the processing of personal data of data subjects 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 such data subjects.

While they consequently have addressed the issue above, they have done so in a manner creating another equally, or at least almost equally, serious issue – it is not clear whether the words 'in the Union' in Article 3(2) relate to 'data subjects' or 'processing'.

The latter alternative is perhaps preferable compared to the former. However, if Article 3(2) is meant to regulate the processing taking place 'in the Union' by a controller or processor not established in the Union, significantly more guidance is desirable than what we have received so far.

As noted, the alternative that 'in the Union' in Article 3(2) relates to the location of the 'data subjects' is plausible. That would mean that the original proposal's limitation to 'data subjects residing in the Union' has been replaced by a location-focused test. In the absence of further limitations, such an approach would seem to bring the Regulation's Article 3 back into the realm of absurdity.

Imagine that a US citizen while in the US signs up for a particular US-based web service which places cookies on that person's browser in a manner that can be seen as 'monitoring' the user. As long as that US citizen remains in the US, no drama arises. However, should that person get on a flight, like many people do these days, and travel to Berlin, Stockholm or some other beautiful place in Europe, then the US web service is suddenly

bound by the European Regulation as soon as that person starts browsing the web. After all, (1) the US company is clearly a 'controller or processor not established in the Union', (2) the US citizen is a data subject 'in the Union' after stepping off the plane in Europe and (3) once she or he starts surfing the web, she/he is 'monitored'.

The scenario described is not fanciful or unusual, and has nothing to do with creating a 'level-playing field' – the key aim of the Regulation's extraterritorial scope. In fact, it demonstrates that, on this interpretation, the Regulation will have an enormously wide scope of application given the mobility associated with modern society – any organisation that reasonably expects to engage with their customers while those customers travel to Europe must seriously consider their position under the Regulation.

The latest installment, at the time of writing, is the Council's proposal (European Parliament 2014). The relevant part reads as follows:

> 3.2 This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
> (a) the offering of goods or services, irrespective of whether a payment by 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 European Union.

This is no doubt the best of the three proposals discussed here. Yet, I am afraid that this solution also falls well short of what is acceptable. To understand why, it is useful to look in more detail at how the Council of the European Union (2014, para. 20) sees this provision work in practise:

> In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where

> the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union (…).

From this, it is clear that the Council is hoping to leverage the 'targeting' approach that has been developed in relation to consumer protection law in Europe, not least through the decision in the joined cases *Pammer v. Reederei Karl Schlüter GmbH & KG11* and *Hotel Alpenhof GesmbH v. Oliver Heller* (C 585/08 & C 144/09, judgment of 7 December 2010).

Drawing upon legal solutions from other fields is sensible, and consumer protection law shares several key features with data privacy law. So far so good. And in addition, several commentators of the highest caliber have been endorsing the 'targeting' approach. For example, in Making Laws for Cyberspace, Reed (2012, p. 225) states that:

> a seller who targets the consumers of a particular state online has clearly joined, albeit temporarily, the trading community of that state. Because of this, the trader is likely to recognize the authority of that state's lawmaker over its transactions, and thus to grant the necessary protection voluntarily.

The problem is that the targeting approach, at least as applied by the Advocate General and the Court in *Pammer/Hotel Alpenhof*, is misguided in that it focuses on the subjective intentions of the relevant party.

Both the Advocate General and the European Court of Justice (ECJ) seem to take the view that the phrase 'directs such activities' implies a conscious decision executed without mistakes. The Advocate General (2010, para. 63) states: 'It is therefore essential for there to be active conduct on the part of the undertaking, the objective and outcome of which is to win customers from other Member States.'

While I agree that there must be some active conduct on the part of the undertaking, the problem with this approach is found in the words in italic. We can have a situation in which the objective of an activity is to win

customers from other Member States, but no such outcome is realised. And we can have a situation in which the outcome of an activity is to win customers from other Member States, without it being the trader's objective. Imagine the following scenario that I (2011, p. 301) have used elsewhere to illustrate this point.

A trader in Greece wishes to carry out an extensive marketing campaign in Switzerland, but miscommunicates its wishes so that the marketing company it has hired is under the impression that the country to be targeted is Sweden. The result is that every Swedish household receives marketing materials from the Greek business, and the Greek business accepts a large number of orders from consumers in Sweden. In such a scenario, the Greek business has never made a conscious decision to direct its activities to the consumers in Sweden. Similarly, it would be incorrect to say that the Greek business envisaged doing business with consumers domiciled in Sweden, in the sense that it was minded to conclude a contract with them prior to any contracts were entered into. Put simply, it was never the Greek business' objective to win customers from Sweden.

Applying the standard set by the ECJ, and promoted by the Advocate General, the Swedish consumers would then not be protected by Article 15(1)(c) of the Brussels I Regulation. Surely this cannot be in line with the intent of the drafters of the Regulation? And surely this is not the type of approach we would like to see adopted for the data privacy Regulation?

The better approach is to distinguish between objective and outcome and only focus on the outcome when determining whether the business has directed its activities to the consumer's state. Such a move from subjectivity to objectivity promotes certainty and fairness.

In the end, however, even with this improvement it is doubtful that the targeting approach will be able to produce good results in the data privacy setting where many instances of data collection and processing will lack reference to the factors, such as currency, meant to determine whether the party targeted Europe or not. Targeting is appealing in theory, but in action on the ground it is likely to be rather useless; it will provide no certainty for the parties involved, and for a large number of parties involved in the handling of personal data, courts are going to have to conclude either that they target just about every country in the world or no countries at all. Both of these options will render the targeting approach useless.

3.2 JURISDICTIONAL LASAGNE TO THE RESCUE

The approach taken to extraterritoriality, both in the current data privacy Directive and in all versions of the proposed Regulation, is binary. All or nothing. If a non-EU business or organisation meets the 'extraterritoriality test', it is bound by the full force of the Regulation.

This unsophisticated approach is problematic. It simply does not make sense to apply the same standard of extraterritoriality to provisions such as Article 5 (requiring e.g. that personal data is processed lawfully, fairly and in a transparent manner), and to Article 35 (demanding the designation of a potentially costly data protection officer). While it may be reasonable to ask a foreign company to abide by a country's rules discouraging or penalising unauthorised and unreasonable disclosure or other use of personal data based on a certain degree of contact between that company and that country (e.g. a transaction involving the collection of personal data), the same degree of contact may not justify that country imposing on the company the duty of designating a data protection officer. The first type of rule is similar in nature to rules found in other areas of law, such as the law of defamation. In a sense, they are private in nature, while rules such as e.g. requiring a data protection officer are of a, comparatively heavy-handed, public law nature.

In an article published in International Data Privacy Law, I (2013b) have put forward a proposal for an alternative approach to delineating the extraterritorial scope of data privacy laws. I will here summarise the key points of that approach.

- Data privacy laws always incorporate a diverse range of legal rules. Thus, it is misguided and naive to think that the same rule of extraterritoriality can be applied to all these types of rules.
- Thus, I propose that we dissect our data privacy law and assign all substantive rules to one of the following three 'layers':
  1. The abuse-prevention layer;
  2. The rights layer; and
  3. The administrative layer.
- As already noted, data privacy laws commonly contain provisions seeking to discourage or even penalise unauthorised and unreasonable disclosure or other use of personal data, in a manner

similar to how e.g. defamation law seeks to prevent abuse. Such rules ought to clearly fall within the abuse-prevention layer.

- Within the rights layer we can comfortably place data privacy rules such as the right of access and the right of correction commonly found in data privacy laws.
- As already hinted at, in the administrative layer, we should place data privacy rules such as the requirements of a designated data protection officer found in the proposed EU data privacy Regulation.
- We can then assign a different extraterritorial test for each layer, with a more restrictive test for layer two than for layer one, and even more restrictive test for layer three.

Experience has taught us that the current approaches to extraterritoriality in data privacy law simply do not work. They are clumsily managing to be both overzealous and inadequate at the same time. Thus, this conundrum must be solved through the development of new approaches, such as the 'layered approach', or 'jurisdictional lasagne', advocated above.

3.3 CONCLUDING REMARKS REGARDING EXTRATERRITORIALITY IN DATA PRIVACY LAW

The above ought to have made clear that, in my view, the overly broad extraterritorial reach of the proposed EU data privacy Regulation is undesirable and destructive. In fact, I would not be surprised if it leads to reactions similar to what we have seen in the context of cross-border defamation law and cross-border anti-competition law where the result has included defensive actions such as:

1. Laws that prohibit the giving of evidence and the production of documents in foreign proceedings;
2. Laws that aims to block or prevent the enforcement of foreign judgments;
3. Laws prohibiting compliance with orders of foreign authorities; and
4. 'Claw-back' laws.

The resulting landscape will be messy indeed and to the detriment of data subjects, data processors and data controllers.

4. THE SO-CALLED 'RIGHT TO BE FORGOTTEN'

While it is my view that the so-called 'right to be forgotten' has gained more attention than it deserves, the temptation to make some observations about this 'right' is too great to be resisted. And indeed as I will show below, due to some ill-conceived Guidelines by the Article 29 Data Protection Working Party on the proper application of the right to be forgotten, the *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) Case C-131/12 has unfortunately taken a turn making it impossible to ignore when dealing with extraterritoriality in data privacy law.

The *Google Spain* case requires no introduction, but in the briefest of terms: when Spanish citizen Mr Mario Costeja González found links to two, for him, unflattering pages of the Spanish newspaper *La Vanguardia* from 1998, he requested that the newspaper remove the personal information about him contained in the relevant pages. He also requested that Google Spain and Google Inc remove or conceal the personal data relating to him so that the data no longer appeared in the search results and in the links to *La Vanguardia*.

The matter ended up before the Spanish data protection authority Agencia Española de Protección de Datos (AEPD). The AEPD rejected the complaint against *La Vanguardia*. At the same time, it upheld the complaint against Google.

Google brought the matter before the Spanish National High Court (Audiencia Nacional), and that court referred the matter to the Court of Justice of the European Union.

The CJEU's decision is legally technical, and many of the legal questions dealt with are specific to the European Union. However, the consequences of the decision are global. For example, the Court discussed in detail whether the functions carried out by Google Search amounted to data 'processing', and whether Google was a data 'controller' under the relevant EU law.

The Court answering both these questions in the affirmative meant that Google was responsible for its search results completely independently of the possible liabilities of the publishers, such as the newspaper in this case.

This means that even if certain content, such as the newspaper reporting relating to Mr Mario Costeja González, can lawfully be uploaded to the Internet, it may be unlawful for Google to list such content in its search results.

For the EU, there are practical advantages in such an approach. It means that, by controlling the search engines, it can affect at least the likelihood of personal information being found online even where the information is provided by a party located outside the EU.

While in line with the approaches taken in the United States, its long-term implications for the Internet may be severely limiting.

4.1 THE POWER OF LABELS

The first thing that strikes me as odd about the right to be forgotten is how a well chosen expression may capture our imagination. 'Cloud computing', 'big data' and the 'right to be forgotten' are all examples of phenomena that existed prior to, but came to life through, the catchy labels we attached to them. Am I the only one worried by this? Isn't there something odd about the idea that the focus of legal, and other, researchers is so strongly guided by something as flimsy as catchy labels?

Fortunately, a catchy label alone may perhaps not be enough; something else may be needed. Looking at the development of research relating to 'cloud computing', 'Big Data' and the 'right to be forgotten', it seems to me that where we have a strongly developing phenomenon (SDP) and a catchy label (CL) describing that phenomenon, we are guaranteed to see significant research interest (SRI):

$$SDP + CL = SRI$$

Perhaps keeping this simple formula in mind may assist us in predicting 'the next big thing'?

It is also interesting to consider how strongly the mental pictures painted by the labels guide our thinking. Labels such as 'going online', 'visiting a website' and the 'web' have all had an impact on how the law, and legal researchers, approach the underlying phenomena – our thinking is shaped by labels chosen perhaps rather arbitrarily and without legal consequences in mind. Also this worries me, and perhaps the time has come to be more careful in this regard.

Below I will argue that the recent judgment of the Court of Justice of the European Union in *Google Spain* cannot be seen to articulate a 'right to be forgotten' but rather a (selective) 'duty to be forgetful'. This difference is not merely a matter of phrasing.

4.2 A 'RIGHT TO BE FORGOTTEN' OR A (SELECTIVE) 'DUTY TO BE FORGETFUL'?

The 'right to be forgotten' has attracted considerable attention for some years now both in legal circles and in media. And as is well-known, much, perhaps too much, of the focus of the undergoing reform work of the EU data privacy framework has been devoted to this right.

The relevant legal landscape in Europe has been largely unaltered since the Data Protection Directive (Directive 95/46) was introduced in the mid-90s. So the thought that the current debate influenced the CJEU's willingness to embrace a right to be forgotten in *Google Spain* is inescapable.

At any rate, even if the Court spoke expressly about a right to be forgotten, it seems to me that that was not what they delivered in their judgment. The court order is not focused on any such right. If it was, it would have required the original publisher (*La Vanguardia*) to remove the content as well, but it did not.

The real effect of the judgment is to impose a 'duty to be forgetful' onto certain Internet actors – in this case search engines, or indeed, one particular search engine.

So does this matter? I think it does. First of all, politically, it is of course always easier to 'sell' a right than it is to sell a duty. And second, as was referred to more generally above, the labels guide, or even control, our thinking to a large extent.

4.3 WHO WILL STAND UP FOR FREEDOM OF EXPRESSION?

The Court concluded that, where search results appear to be inadequate, irrelevant or no longer relevant, or excessive, the information and links concerned in the list of results must be erased. This applies even where the information is true and published lawfully by third parties. In other words, the Court places on Google the burden of deciding whether search results have become outdated.

In response to the decision, search engines such as Google and Bing have set up facilities allowing people to request the removal of certain search results. Large numbers of people have taken up this option.

The latest reported figures from Google show the search giant has received more than 174,000 requests on 602,000 links, of which 41.5% have been removed from European search results following evaluation (Kelion 2014).

The practical difficulties with this blocking are obvious. First of all, there is the risk of search engines erring on the side of caution and removing any content complained of. After all, the risks of not removing the content may easily outweigh any perceived advantage of keeping the content accessible. Second, content may be seen to be outdated and irrelevant on one date only to become highly relevant again at a later date.

For example, information about a person's conduct may be seen to be outdated one day but become relevant again at a later date if that conduct is repeated. In other words, the relevance of information is not static – it is constantly changing and is always dependent on context.

Imagine that a person kills someone, then serves time in jail and upon release requests blocking of information relating to the murder. If that same person kills again, the old blocked reporting of the first murder must be seen as relevant again, but who will take on the role of ensuring that it is unblocked?

In any case, the Court's conclusion on the right to be forgotten will no doubt reverberate across the world. Indeed, it forces the creation of a more forgetful Internet.

From a privacy perspective this must be seen as a victory. But at the same time, privacy interests must always be balanced against competing interests such as freedom of information. The Court (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) Case C-131/12 at para. 100) acknowledged this and stated that, while the right to be forgotten ordinarily trumps competing interests such as the economic interest of the search engine operator and the interest of the general public in finding information upon a search relating to the data subject's name:

> That would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public

> life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

The question is of course how this assessment will work in practice.

4.4 THE EXTRATERRITORIAL DIMENSION OF THE 'RIGHT TO BE FORGOTTEN'

The Article 29 Data Protection Working Party's Guidelines (2014) regarding the Google Spain decision emphasise that:

> [i]n order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented.
>
> In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.

Thus, the message is clear: the Article 29 Data Protection Working Party wants global blocking so as to ensure that EU law is not 'circumvented'. The question is of course whether blocking on the .com domain will be enough to achieve this.

The reasoning behind blocking on the global .com domain is that it is easy for people to use google.com to access content blocked on a country-specific search such as google.es – the Spanish domain.

But, if content is blocked also on google.com, will not people who are sufficiently motivated to search for the content simply use another country-specific search such as google.com.au?

After all, doing so only requires the pressing of three extra keys – '.au'. Will this reasoning then mean that to comply with EU law, search engines

need to block search results all over the world? Where do we pull the brake and say enough is enough?

The Article 29 Data Protection Working Party's attempt to impose global blocking based on local values should not be seen in isolation. Other countries are doing exactly the same thing. For example, the US is doing so in *Garcia v. Google, Inc.*, 743 F.3d 1258 (9th Cir. 2014), amended by *Garcia v. Google, Inc.*, No. 12-57302, 2014 WL 3377343 (9th Cir. July 11, 2014) (Svantesson 2014a), and Canada does so in *Equustek Solutions Inc v. Jack*, 2014 BCSC 1063 (Svantesson 2014b).

This attitude may be seen as natural and may even be viewed as necessary by some; after all, the most effective way to ensure that content cannot be accessed is through global blocking. But the problems caused by this attitude abound.

Most importantly, if our standard position is global blocking based on our local laws, we can hardly object to other countries doing the same. So when oppressive dictatorships seek global removal of content offensive to their laws, supporters of the Article 29 Data Protection Working Party's Guidelines can hardly protest based on the effect such removal may have in open tolerant and democratic states.

The reality is that the trend of states demanding global blocking based on local laws will inevitably lead to the destruction of a common resource – the Internet as we know it. What would be left online if anything that may be unlawful somewhere in the world was removed globally?

Addressing this trend may be both the biggest, and the most important, challenge for Internet regulation today.

5. BIG DATA – DOES SIZE REALLY MATTER?

The most interesting current and future development in the data privacy sphere is no doubt the development of Big Data and the Internet of Things. Information and communication technologies, or ICT, make possible the collection, storage, use and distribution of data on a previously unimaginable scale. And with increasing storage and processing power in ever smaller devices, combined with increased connection speeds, it can be anticipated that data collection, storage, use and distribution will only continue to increase.

Lately, 'Big Data' has become a term of art referring to 'novel ways in which organisations, including government and businesses, combine

diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations' (Rubinstein 2013, p. 74).

Just how large quantities of data we are dealing with is clear from the below:

> The *Economist* reports in its 2012 Outlook that the quantity of global digital data expanded from 130 exabytes in 2005 to 1,227 in 2010, and is predicted to rise to 7,910 exabytes in 2015. [internal footnote omitted].
>
> An exabyte is a quintillion bytes. If you find that hard to visualize, consider this: someone has calculated that if you loaded an exabyte of data on to DVDs in slimline jewel cases, and then loaded them into Boeing 747 aircraft, it would take 13,513 planes to transport one exabyte of data. Using DVDs to move the data collected globally in 2010 would require a fleet of more than 16 million jumbo jets (Kuner et al. 2012).

Where large quantities of data are being stored, such collections may, depending on the type of data, become 'honey pots' targeted by parties wanting to gain access to the data in question. Typical examples of honey pots include databases that include credit card information, user details, passwords etc. In other words, size is a problem in itself when it comes to data management, and perhaps it could be said that the larger the data collection the more attractive it is to third parties and, therefore, the more at risk it is.

Leaving aside the 'honey pot' issue, one key privacy issue with Big Data is neatly described in a paper released by the White House: 'Computational capabilities now make "finding a needle in a haystack" not only possible, but practical. [...] A key privacy challenge in this model of discovery is that in order to find the needle, you have to have a haystack. To obtain certain insights, you need a certain quantity of data' (Executive Office of the President 2014, p. 6-7).

And related to this we can identify another important data privacy consideration:

> The data clusters and relationships revealed in large data sets can be unexpected but deliver incisive results. On the other

> hand, even with lots of data, the information revealed by big data analysis isn't necessarily perfect. Identifying a pattern doesn't establish whether that pattern is significant. Correlation still doesn't equal causation. Finding a correlation with big data techniques may not be an appropriate basis for predicting outcomes or behavior, or rendering judgments on individuals. In big data, as with all data, interpretation is always important (Executive Office of the President 2014, p. 7).

Put simply, decision-making based on Big Data may be a recipe for misguided, unfair and discriminatory outcomes.

A development related to the Big Data revolution is the so-called Internet of Things:

> The 'Internet of Things' is a term used to describe the ability of devices to communicate with each other using embedded sensors that are linked through wired and wireless networks. These devices could include your thermostat, your car, or a pill you swallow so the doctor can monitor the health of your digestive tract. These connected devices use the Internet to transmit, compile, and analyze data (Executive Office of the President 2014, p. 2).

I will not discuss the Internet of Things in detail. It suffices to note that when even your toaster, washing machine and your own body are spying on you, protecting privacy will be even more difficult, and even more important.

6. THE FAIRYTALE CONCEPT OF 'CONSENT' VS. A 'NANNY STATE' APPROACH

Most of us can probably agree upon some suitable definition of the concept of 'consent'. Our definition would probably refer to things like consent being given in some identifiable form, that it be sufficiently informed and given freely. And in some legal areas the concept makes sense and fills a function. However, I am afraid that data privacy is not such an area.

In fact, as far as data privacy is concerned, 'consent' is, as I (2012) have been arguing for some years, quite simply a fairytale concept. Thus, the fact that we can describe, define and delineate what we mean by consent does

not make it any more real than unicorns and mermaids – those things can also be described, but we all know they are not real.

So why this skepticism towards consent? Well, the reality is that people give their consent to so many different things on a daily basis without any real consideration. Is consent *informed* when you click 'I agree' to a 50-page legal document just to access a certain website? And is consent *given freely* when you agree to the terms of use for software you necessarily need to function in the workforce? The obvious answer to both these questions is, 'No'.

I am by no means alone in my skepticism towards the concept of 'consent'. In fact, nothing I have said above is particularly controversial. The problem, and the reason why we still rely on consent, is that it is difficult to think of an alternative to relying on consent. Here I will canvass one possible, be as it may a not entirely attractive, alternative.

One possibility is that we move towards what in derogatory terms could be referred to as 'nanny state data protection'. Despite the negative term, such an alternative may not be all bad, and inspiration could be drawn from the EU Directive on unfair contracts terms from 1993. The approach taken in that Directive could be seen as a step away from party autonomy and self-determination in that, whatever may be the genuine wishes of the parties, it prevents certain types of contract terms from being included in certain types of contracts under certain conditions.

One can easily picture a similar 'nanny state' approach in data privacy law, which would mark a departure from a largely consent-based paradigm of informational self-determination. The advantages are obvious. For example, if the rules in question are carefully drafted, they may provide a clearer guidance for businesses and other organisations handling personal data. Further, and most importantly, we would no longer need to rely on the fairytale like notion of 'genuine consent'.

7. CONCLUDING REMARKS

In the above, I have sought to draw attention to a selection of legal issues that arise in the context of data privacy. Had my intention been to paint some sort of coherent picture, the above would have been an obvious failure. Fortunately, I had no such grand aims. However, in bringing attention to the need for Europe to broaden its perspective to take account, to a greater extent than presently is the case, of what goes on in the data

privacy landscape around the world, I hope to have achieved something of value. And in discussing the significance of the extraterritoriality of data privacy law, I hope (perhaps in vain) to bring attention to the danger of the path the EU is taking. Further, perhaps what is said above about the right to be forgotten, big data and the Internet of things can be of some interest.

So what does the future hold for data privacy? The only thing that is clear is that data privacy is not a fad that will go away any time soon. I have no doubt the debate about data privacy will intensify rather than die down. And wherever that debate takes us, we need to remember that data privacy is a fundamental human right. It is then not good enough to conclude that privacy is dying, dead or, indeed, a zombie.

To say that we do not need a right of privacy because our modern information society does not cater for privacy is akin to saying that we do not need a right to water in a desert – the removal of a fundamental right is justified by reference to the environment being hostile to, or making difficult the exercise of, such a right. Such reasoning is clearly flawed and the opposite is clearly correct – the right to water is much more relevant in a desert than in a champagne bar in Paris. Similarly, the right to privacy is more important in our current privacy-hostile technological environment than it ever has been before.

In light of this, data privacy – the 'ugly duckling' of the human rights – is more likely to continue to develop in importance than it is to become irrelevant.

LIST OF REFERENCES

Advocate General Trstenjak 2010, Opinion of Advocate General Trstenjak delivered on 18 May, Case C-585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Case C-144/09 Hotel Alpenhof GesmbH v Oliver Heller, 18 May, <http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=79076&cid=594463>.

Article 29 Data Protection Working Party 2014, Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos

(AEPD) and Mario Costeja González" c-131/121, 26 November, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

Bogdan, M 2005, 'Is there a curricular core for the trans-national lawyer?' Journal of Legal Education, vol. 55, pp. 484-87.

Council of the European Union 2014, proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Partial General Approach on Chapter 5, 28 May.

European Commission 2014, Progress on EU data protection reform now irreversible following European Parliament vote, memo/14/186, Strasbourg, 14 March <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm>.

European Data Protection Supervisor 2012, Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March, <http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf>.

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Executive Office of the President 2014, Big Data: Seizing Opportunities, Preserving Values, 1 May

<http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014) Case C-131/12.

Greenleaf, G 2014, 'South Korea's innovations in data privacy principles: Asian comparisons', Computer Law&Security Review, vol. 30, p. 492-505

Kelion, L 2014, Google told to expand right to be forgotten, BBC News Online, viewed 5 January 2015, <http://www.bbc.com/news/technology-30212927>.

Koops, B-J 2014, 'The trouble with European data protection law', International Data Privacy Law, vol. 4, no. 4, pp. 250-61.

Kuner, C, Cate, FH, Millard, C & Svantesson D 2012, 'Editorial: The Challenge of "Big Data" for Data Protection', International Data Privacy Law, vol. 2, no. 2, pp. 47-9.

Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) 25.01.2012. COM(2012) 11 <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011>.

Reed, C 2012, Making Laws for Cyberspace, Oxford University Press, Oxford.

Reding, V (European Commission Vice President, EU Justice Commissioner) 2014, The EU data protection Regulation: promoting technological innovation and safeguarding citizens' rights, Intervention at the Justice Council, European Commission, Brussels, 4 March <http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved

=0CB0QFjAA&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_SPEECH-14-175_en.pdf&ei=dXqPVMbDJOfDmAXvjoGwBQ&usg=AFQjCNFaKeWXeENxaXcG8YamoqhkayhGcQ&bvm=bv.81828268,d.dGY>.

Rubinstein, IS 2013, 'Big Data: The End of Privacy or a New Beginning?' International Data Privacy Law, vol. 3, no. 2, p. 74.

Svantesson, D 2011, 'Pammer and Hotel Alpenhof – ECJ decision creates further uncertainty about when e-businesses "direct activities" to a consumer's state under the Brussels I Regulation', Computer Law & Security Review, vol. 27, no. 3, pp. 298-304.

Svantesson, D 2012, Online workplace surveillance—the view from down under, Privacy in the Workplace, Pécs Hungary, April, <http://pawproject.eu/en/sites/default/files/page/12_svantesson_workplace_surveillance.pdf>.

Svantesson, D 2013a, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing, Copenhagen.

Svantesson, D 2013b, 'A "layered approach" to the extraterritoriality of data privacy laws', International Data Privacy Law, vol. 3, no. 4, pp. 278-86.

Svantesson, D 2014a, Innocence or arrogance? US court oversteps on internet regulation, The Conversation, 7 April <https://theconversation.com/innocence-or-arrogance-us-court-oversteps-on-internet-regulation-25215>.

Svantesson, D 2014b, The Canadian 'Google case' – B.C. imperialism or a legitimate response to a difficult issue? LinkedIn article, 28 August <https://www.linkedin.com/pulse/20140828080321-308862488-the-canadian-google-case-b-c-imperialism-or-a-legitimate-response-to-a-difficult-issue>.