Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein

Martin Scheinin

Introduction

Much has already happened since the 6 October 2015 CJEU Grand Chamber ruling in *Max Schrems*.[1] A case commentary by Tuomas Ojanen is included in this issue. The political ramifications have involved a wide range of actors on both sides of the Atlantic Ocean. Data has not stopped flowing, and on the political level we may have a new deal on how to let it flow also in the future, the so-called Privacy Shield arrangement.[2] The blogosphere and academia have not stopped discussing the implications of the *Max Schrems* ruling, and critics have already voiced their view that Privacy Shield may be subject to new litigation and would be unlikely to stand the test established in *Max Schrems* if the case ultimately makes its way back to the European Court of Justice.[3] We are reminded of the *Kadi* saga, in which the political organs of the EU chose to renew the terrorist listing of Mr Kadi, knowing full well that this would result in a lengthy new round of litigation before the Court of First Instance and the European Court of Justice. In *Kadi*, the strategy worked, at least on some levels, as ultimately there was political consensus about the delisting of Mr Kadi at the United Nations Security Council level before the European Court of Justice got a chance to quash the EU-level relisting decision. At no point was there either a situation where the EU would have failed to comply with its obligations under international law — pursuant to Chapter VII of the UN Charter — or of the European Court of Justice failing to perform its task of being the guardian of fundamental rights internally within EU law. Maybe in a

[1] ECJ 6 October 2015, Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*.

[2] <www.politico.eu/article/the-phone-call-that-saved-safe-harbor-john-kerry-frans-timmermans/>, visited 22 June 2016.

[3] <arstechnica.co.uk/tech-policy/2016/02/interview-safe-harbour-2-0-will-lose-again-argues-max-schrems/>, visited 22 June 2016.

European Constitutional Law Review, 12: 341–348, 2016

doi:10.1017/S1574019616000201

couple of years from now professors will also be including the *Schrems* saga in our course syllabi.

My take on the case

Before providing my comments on Richard A. Epstein's provocative critique of what may one day be referred to as *Max Schrems I*, I wish briefly to outline my own take on the European Court of Justice ruling, based on my early comment on the Verfassungsblog.[4] Tuomas Ojanen has a more extensive case analysis elsewhere in this issue, so I am limiting myself to a couple of highlights.

The 6 October 2015 European Court of Justice Grand Chamber ruling in *Max Schrems* tells us much about the status of two fundamental rights in the EU legal order, namely the right to the respect for private life (privacy) and the right to the protection of personal data (Articles 7 and 8 respectively of the EU Charter of Fundamental Rights). The ruling must be read together with the 8 April 2014 ruling in *Digital Rights Ireland,* where Articles 7 and 8 were discussed side by side. Although the subsequent *Max Schrems* ruling contains many references to personal data, it does not really discuss the right to the protection of personal data as a distinct fundamental right. Article 8 of the Charter is mentioned in the dispositive part of the ruling but not, for instance, in what I see as the main finding by the Court, which refers only to Article 7:

> In particular, legislation permitting the public authorities to have *access* on a generalised basis to the *content* of electronic communications must be regarded as compromising the *essence* of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter… (paragraph 94, emphasis added)

The outcome of the case – declaring Commission's Safe Harbor Decision 2000/52 invalid – flows from this finding of a breach of the essence of the right to privacy when we are dealing with indiscriminate blanket access to data. In *Digital Rights Ireland,* the European Court of Justice had already indicated that blanket access to 'content' would trigger the application of the essence clause in Article 52 (1.1) of the Charter, while surveillance, even indiscriminate mass surveillance, based on even complex use of various categories of metadata amounted to a 'particularly serious interference' with fundamental rights but did not trigger the application of the essence clause. The Court's distinction between 'content' and 'metadata' can be criticised, and it was indeed relativised by the Court itself in *Digital Rights Ireland*. But that ruling created a clear expectation that, once seized with a case

[4] <verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion/>, visited 22 June 2016.

https://doi.org/10.1017/S1574019616000201 Published online by Cambridge University Press

where mass surveillance extends to content data, the European Court of Justice would consider that the essence of privacy was at issue.

This is exactly what then happened in *Max Schrems*: the Court actually identified the intrusion in question as falling under the notion of the essence of privacy – something the European Court of Human Rights has never done under the privacy provision of Article 8 ECHR. Consequently, the identification of an intrusion as compromising the essence of privacy meant that there was no need for a proportionality assessment under Article 52 (1.2) of the Charter. This can again be contrasted with the *Digital Rights Ireland* judgment, where the final outcome was based on the application of a proportionality test. For these reasons, the *Max Schrems* judgment is a path-breaking development, a major contribution to the understanding of the structure and legal effect of fundamental rights under the Charter. *Digital Rights Ireland* indicated where the path would go, and now the Court actually went that way.

Besides the words 'essence' and 'content', the above quote from paragraph 94 of the *Max Schrems* ruling also highlighted the word 'access'. Mere 'access' by public authorities to personal data such as electronic communications constitutes an interference with privacy. Surveillance advocates might have, until the *Max Schrems* ruling, enjoyed some credibility with their claims that mere access does not amount to 'processing' of personal data, and therefore mere access to the flow of communications does not amount to an intrusion until the moment when automated selectors and algorithms have done their job and the human eye starts to 'process' a much more narrow set of data. Now we know that mere access is an intrusion into privacy, and even into the essence of privacy when it provides for indiscriminate access to 'content'.

The factual basis of the *Max Schrems* case, subject to litigation before Irish courts, related to the transfer of data from Europe to servers in the United States. The European Court of Justice was asked a question about data transfers from Europe to Facebook servers in the US under the Safe Harbor arrangement, and it responded to that question. It did not address the scenario of 'upstream' access to data flows through the splitting of fiber-optic cables to obtain generic access to all data that passes through transatlantic cables, just because the internet is built in the way that a lot of traffic ends up going through those cables. Nevertheless, paragraph 94 quoted above is formulated in a way that gives a generic answer concerning the contours of the right to privacy under Article 7 of the EU Charter: indeed, access through the upstream method of capturing the data flow in a fibre-optic cable is also to be regarded as compromising the essence of privacy and therefore as prohibited under the Charter, without a need even to engage in a proportionality analysis. After the European Court of Justice's ruling in *Max Schrems,* the content of the substantive norm under Article 7 of the Charter has become clear.

https://doi.org/10.1017/S1574019616000201 Published online by Cambridge University Press

My big disagreements with Epstein

Let me now move to a rejoinder to the contribution by Richard A. Epstein. His opening paragraph presents a seemingly compelling narrative that will frame the mindset of the reader: in October 2015, the European Court of Justice issued its *Max Schrems* ruling in such a mundane matter as someone's Facebook information, oblivious to the fact that just one month later ISIS terrorists would storm Paris and slaughter 130 innocent people. The link between the two? Oh yes, according to Epstein it is 'widely understood' that the ISIS operatives in Paris were able to 'communicate under the radar', 'often with encrypted devices', so that the attack 'came as a complete surprise to public authorities'. To me, this is a nice try to prepare the reader for Epstein's frontal attack on the *Max Schrems* ruling. The problem is that what he writes about the Paris attack is blatantly not true. If the France- and Belgium-born attackers communicated under the radar, it was because they knew each other personally, having grown up in the same suburbs. When they used electronic means of communication, they relied on unencrypted mobile phones and even boasted about their plans on Facebook – yes, ironically — Facebook. And many of the attackers were known to the French or Belgian authorities, who just had too many leads to follow. The fact that the attack came as a surprise demonstrates a failure of intelligence coordination internally in France and in Belgium, and between those two neighbouring EU countries. More broadly, it demonstrates a failure of the collect-it-all mentality, whereby any unmonitored modalities of communication are seen as an unknown security threat worth any investment of money, personnel and political influence – often to the detriment of taking action in respect of known security threats, such as individuals already suspected of preparing acts of terrorism.

Besides disagreeing about the facts, I also disagree with Epstein about the law. His piece demonstrates an approach to law and courts that is at odds with how we tend to address these issues in Europe. According to him, the European Court of Justice showed 'massive indifference' to the particulars of American law when it struck down Safe Harbor. No, it was an issue of jurisdiction. The European Court of Justice is an internal EU court operating under EU law and, in particular, reviewing that EU organs do not overstep their lawful competences as provided by the Member States in the Treaties and in secondary legislation enacted pursuant to the Treaties. When deciding and agreeing on Safe Harbor, the Commission had in important ways disregarded the rules of EU law that safeguard the fundamental right to privacy. Hence, the Commission's action was declared unlawful, irrespective of what changes there perhaps had been in US law after the facts of the case had been presented to an Irish court, which in turn had sought the legally binding resolution of an EU law issue from the European Court of Justice.

According to Epstein, 'the entire fuss over privacy' in the European Court of Justice ruling is 'somewhat of a mystery' to him. And so it probably appears,

if one's understanding of privacy is based on what Warren and Brandeis wrote in 1890 and on the assumption that mass collection of personal data does not constitute an invasion of privacy until 'actual harm' is proven in an individual case. What remains mysterious to Epstein is that under the European Convention of Human Rights and the EU Charter of Fundamental Rights, the collection of personal data by a public authority certainly already is 'actual harm' in the sense that it constitutes an interference with the person's right to the protection of private life and right to the protection of personal data. In fact, that level of actual harm is triggered *earlier* than at the stage when public authorities *collect* personal data: it is triggered when they have *access* to data, for instance when it is retained by private actors such as Facebook or telecommunications providers so that public authorities will have access to it. This is the crux of the matter in the European Court of Justice rulings in *Digital Rights Ireland* and *Max Schrems*. Laws that give to public authorities, such as the police or intelligence agencies, access to telephone call logs, e-mail logs, internet browsing records, Facebook user information, or the content of e-mails, *all* constitute interferences in privacy rights by their mere existence.

Why this may appear a 'mystery' to some US scholars is because the fact that something constitutes an interference with a human or fundamental right does not mean that it automatically would be a *violation* of that right. A number of considerations must be taken into account when determining whether an interference indeed is a violation of privacy or, instead, a *permissible limitation*, i.e. a lawful restriction. Among the cumulative conditions that an interference must meet in order to be permissible are that it must not breach the essence of the right in question, there must be a proper legal basis for the interference, and the interference must effectively serve a legitimate aim so that it can be deemed as necessary in a democratic society. After all these tests have been met, it still needs to be attested that the resulting intrusion remains proportionate in relation to the actually obtained benefit towards delivering the legitimate aim that was used to justify the interference.

The last element – proportionality – was decisive in *Digital Rights Ireland*. Many laws authorising mass surveillance, even in the form of 'mere' access to personal data and hence before actual collection or processing of the material, and even when we deal with so-called metadata or in particular combined categories of metadata, will be deemed to breach the proportionality principle under European standards, be it under the ECHR or the EU Charter. This is how Europe 'strikes the balance' – not as an abstract comparison between the importance of two values, such as privacy versus security, but through a concrete assessment of what actual benefit was gained towards better security and whether that level of benefit overweighs the smallest possible but unavoidable degree of intrusion into privacy.

The first element – the categorical protection of the essence of a fundamental right – was decisive in *Max Schrems*. As the Safe Harbor arrangement resulted in

general access to the 'content' data of individuals, it engaged the essence of the right to privacy, and the intrusion hence was deemed impermissible even without a need to conduct a proportionality assessment. The latter would have become pertinent only further down the road, should the other conditions for a permissible limitation have been present.

Epstein's discussion about the actual rate of 'abuse' in the practice of intelligence agencies is totally off the mark. The collection of the data, and even earlier than that, the access to the data, is already an intrusion – without any requirement of bad faith or abuse. What to Epstein is the 'exact mistake' by the European Court of Justice, namely a 'categorical claim that collection of data counts as mass surveillance', is actually the *law* that the Court is obliged to apply.

A broader issue that highlights, and perhaps explains, Epstein's misperceptions of the protection of human rights and fundamental rights in Europe is his presumption that some fundamental rights could be classified, and then dismissed, as being trivial: 'An invasion of privacy is small potatoes in comparison with the loss of life and limb'. It is true that two human rights may sometimes clash with each other, such that a careful determination must be made as to how to secure compliance with both of them. The category of permissible limitations, and the proportionality assessment as its final stage in many but not all cases, is central in that process. But no fundamental right will be declared as 'small potatoes' in comparison to another one, even in comparison to the right to life as a sacred human right. Proven actual benefit towards safeguarding the right to life does justify intrusions into the right to privacy that are minimised to what is necessary in a democratic society and deemed proportionate in comparison to the benefits obtained, as long as this assessment is made without trivialising the value of the right to privacy as a human and fundamental right.

We need evidence-based discussion on surveillance

I will now move to what I find as the most interesting part of Epstein's critical discussion of the European Court of Justice ruling. He states:

> No defender of general government surveillance programs should favor tactics that are counterproductive, or even those which are not cost effective. At the same time, privacy defenders must concede that some surveillance that government demands is not a waste of time.

Here we have common ground for a proper discussion. What is badly needed is an evidence-based discussion on what methods of surveillance work, and which methods do not produce any real security benefit. And concerning the methods

https://doi.org/10.1017/S1574019616000201 Published online by Cambridge University Press

that do work, we need an assessment of cost-effectiveness. Only then will it be possible to enter into a fully informed discussion on the impact upon privacy and other fundamental rights of those methods of surveillance that are worthy of a proper proportionality assessment: what is the remaining level of privacy intrusion after all adequate measures have been taken to minimise it, including by securing that the essence of the right remains protected? Can that level of intrusion be deemed proportionate in comparison to the proven security benefit obtained at an acceptable financial cost? These are the questions that must be asked to determine whether a particular form of surveillance is permissible in a given context.

This is exactly what we sought to prepare the ground for, and partly do, in SURVEILLE, a three-and-a-half-year multidisciplinary research project funded by the EU through its Seventh Framework Programme for development and research.[5] With reference to the methodology and the findings of the project I am willing to 'concede' that some surveillance that governments want is not a waste of money or time but, on the contrary, is a good investment of resources so that the resulting unavoidable intrusion into privacy rights is kept at a bearable level, always proportionate in comparison to the actual obtained security benefit and never compromising the essence of privacy. In the same breath, I have to state that while I agree with Epstein that no government *should* be pushing for surveillance methods that are counterproductive, far too many governments are in fact pursuing maximalist surveillance agendas without proper evidence-based assessment of the actual benefits of what is proposed, without an honest cost efficiency analysis and without real privacy impact assessment. This is the tragedy of the current surveillance debate.

Many factors can be listed as reasons for the tragedy. One of them is fear amongst politicians who almost at any cost seek to avoid being held politically accountable for the loss of life through a terrorist act. Due to this fear, they are likely to approve any laws or measures presented in the name of security, even without an evidence-based assessment. They are also likely to pass the buck to 'experts' of surveillance and intelligence who in turn may be badly misguided by traditions of secrecy and unaccountability, an unfounded collect-it-all mentality and the lure of what can be named the surveillance-industrial complex that provides lucrative business opportunities to many people, including former government and intelligence officials.

In SURVEILLE, we sought to help find the best methods of surveillance. We applied a scenario-based approach and relied upon three parallel teams of experts

[5] <surveille.eui.eu>, visited 22 June 2016: Surveillance: Ethical Issues, Legal Limitations, and Efficiency, grant agreement no. 284725, for the period 1 February 2012 to 30 June 2015. The reader is instructed, in particular, to consult the SURVEILLE Briefing Note and SURVEILLE deliverable D4.10, both available on the project website. Work towards proper academic publications is in progress.

in order to assess the technological usability, the cost efficiency, the fundamental rights intrusion and the ethical concerns of a range of surveillance techniques and technologies in different situations. Our main finding was that methods of electronic mass surveillance failed the test, as they produced wide and deep privacy intrusions with very low security benefit. Methods of targeted electronic surveillance performed much better, and so did traditional methods of policing and human intelligence. A key question in an evidence-based discussion on surveillance is what alternatives there are to electronic mass surveillance for the proper identification of subjects for targeted surveillance. The collect-it-all mentality failed in Paris, and SURVEILLE research suggests that it will also fail generally. This is partly because electronic mass surveillance tends either to breach the essence of privacy or to result in a disproportionate intrusion on privacy.

https://doi.org/10.1017/S1574019616000201 Published online by Cambridge University Press