The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices

Richard A. Epstein*

THE ECJ BOMBSHELL

On 6 October 2015,[1] the European Court of Justice responded to a claim by the Austrian Maximillian Schrems, who feared for the security of his Facebook information. In response to that claim, the European Court of Justice held that 15-year-old 'safe harbour' provisions governing relations between the United States and the European Union were 'invalid' under the EU's standards because they did not provide 'adequate protection' for the EU data stored and used in the United States. A little over a month later, on 13 November, ISIS terrorists stormed several key locations in Paris and slaughtered some 130 innocent people, injuring hundreds more. It was 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.

The obvious question to ask about this situation is whether the two events are in any meaningful sense related to each other. In one sense the answer should be put into the negative. The European Court of Justice decision was only about the transmission of key datasets into the US. It was not, on its face, about how the US should conduct its internal operations. But that purported separation turns out to be artificial at best. The European Court of Justice decision gave no grace period for implementing the reforms, and it concluded, without any examination of how

*Laurence A. Tisch Professor of Law, The New York University School of Law, Senior Fellow, The Hoover Institution, and the James Parker Hall Distinguished Service Professor of Law Emeritus, and Senior Lecturer, The University of Chicago Law School. My thanks to Craig Fligor and Manuel Valle, The University of Chicago Law School, Class of 2017, for their excellent research assistance.

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

European Constitutional Law Review, 12: 330–340, 2016

doi:10.1017/S1574019616000195

they operated in practice, that the American reforms that had been put into place were per se inadequate. The point is deeply ironic given that the US enacted the United States Freedom Act in the summer of 2015, which introduced what everyone on both sides[2] of the debate agreed were major changes in the structure of the United States' surveillance. That legislation included a 180-day transition period,[3] which allowed for a more limited collection of metadata, and that provision expired on 28 November 2015, which means that mass data collection in the US is at a temporary halt. These events highlight the massive indifference that the European Court of Justice showed to the particulars of American law.

Whither privacy

That stark conclusion stemmed from the European Court of Justice's categorical view that stringent protections were needed to protect individual privacy, which the American law in all its variation failed to provide. In one sense the entire fuss over privacy is something of a mystery. Historically, the law offered its protection to personal liberty, chiefly against physical invasion. It also gave individuals protection for information that they created, like trade secrets, which they could in turn share with others under confidentiality agreements. But privacy as a free-floating interest came relatively late in the day with the famous 1890 article, 'The Right to Privacy',[4] in which Samuel Warren and Louis Brandeis mainly urged that individuals have the right to keep the press from prying into their personal affairs. This position, however, has largely been eviscerated by the acceptance of the modern newsworthiness position.

Yet the protection of privacy has developed a second life in connection with claims of individuals that they are entitled to keep their personal data out of the hands of both business and government. That attitude was strongly evident in the European Court of Justice's decision because it gave little weight to the fact that the relevant data so critical for maintaining routine personnel records, including salary information, had been freely transferred for 15 years under the EU/US agreement. The decision of the European Court of Justice created massive dislocations in the practices of some 4,500 companies—including such stalwarts as Apple, Facebook, and Google—that have routinely relied on the standard practices. Since that time, efforts have been made to organise alternative routes for

[2] S. Siddiqui, 'Congress passes NSA surveillance reform in vindication for Snowden', <www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden>, visited 22 June 2016.

[3] Public Law 114-23, 2 June 2015, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015.

[4] S.D. Warren and L.D. Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* (1890) p. 193.

processing this vital information, but, as of this writing, it seems clear that the widely different views on the importance of privacy and national security have blocked[5] any unified solution to the problem. Therefore, individual firms have been forced to adopt ad hoc responses to this matter, all the while facing serious civil and criminal penalties[6] from European authorities as of January 2016.

In making its decision, the European Court of Justice set aside the initial determination of the EU's Data Protection Commissioner, who had dismissed Schrems's complaint seeking termination of the data collection program. To see where the European Court of Justice has gone off the rails, it is instructive to compare that court's approach with the Commissioner's. The first question that the Commissioner asked was whether Schrems could show that any data he had placed on Facebook Ireland had been compromised when it was thereafter transferred and stored in the US. The Commissioner insisted that, unless Mr Schrems could show some particularised harm to himself, he was not in position to challenge the overall operation of this system, which was in compliance with Decision 2000/520 of the Commission, which set out the basic norms over data collection.

As a matter of general jurisprudence, the Commissioner's approach was eminently sensible because it did not put at risk long-term structures in the absence of any demonstration of actual harm. The point is of great importance in this context, given the heavy reliance of all major data countries on a protocol that had been in place for a long period of time. It is in general a good maxim of law, in the EU as in the US, that 'if it ain't broke, don't fix it.' At this point, the correct question to ask about the US data collection system was the level of actual protection that it afforded. In dealing with this issue, government officials insist that what matters is the level of exposure from the collection of mass data, which in and of itself does not count as an invasion of privacy. As reported in the *Guardian*,[7]

> Privacy campaigners counter that [claim about mass collection] just by having access to such huge volumes of data on every individual citizen amounts to mass surveillance and an invasion of privacy. They also argue that even if the agencies are

[5] M. Gyves, 'German DPAs Announce Policy Severely Limiting Mechanisms for Lawful Germany-to-U.S. Data Transfers', <privacylaw.proskauer.com/2015/10/articles/european-union/german-dpas-announce-policy-severely-limiting-mechanisms-for-lawful-germany-to-u-s-data-transfers/>, visited 22 June 2016.

[6] A. Bywater et al., 'WP29 Lays Down Enforcement Gauntlet', <www.corderycompliance.com/wp29-lays-down-enforcement-gauntlet/>, visited 22 June 2016.

[7] E. MacAskill, 'The NSA's bulk metadata collection authority just expired. What now?', <www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act>, visited 22 June 2016.

> not looking at content – listening to phone calls – they can build up a detailed profile of an individual just on the basis of who was called, the location, time and length of call.

On this issue, I think that the intelligence services have the better of the arguments on both points. In dealing with the direct access to data, the actual rate of abuse has much to do with the desirability of the overall scheme. If these leaks took place on a daily basis, the abuses of privacy would be clear. But if they happened only on rare occasions, the concern is much less. The next question to ask is how quickly government authorities remedy any mistake that has been made in the use or release of data. If these are done promptly, then again the risk to privacy is surely much less than if the information is allowed to circulate freely throughout the world. I am not aware of any system of risk analysis that ignores both the probability and severity of a particular wrong in deciding the level of precautions that should be taken against the adverse event. Yet the European Court of Justice makes this exact mistake in its categorical claim that collection of data counts as mass surveillance.

On the second point, it is surely the case that the ability to trace connections among various parties does allow the government to build up profiles against individual persons—which is of course exactly why the data is collected. If it can be said that piecing together disconnected bits of information allows the government to spy on innocent people, then it should be conceded that the same techniques allow the government to spy on individuals who do pose a threat to the security of other individuals. It seems very odd to say that a technique that is effective in committing privacy violations against ordinary citizens is of no use in tracking terrorists. And given the complete breakdown of intelligence with respect to the perpetrators of the terrorist acts in Paris, it seems that this concern should be greater today than it was at the time of the 6 October decision.

What was true at that time, and is still true today, is that an invasion of privacy is small potatoes in comparison with the loss of life and limb. Even if one thought that the likelihood of privacy abuses was higher than a terrorist attack, the balance should still be tipped clearly in the opposite direction, given the relative severity of the two threats. In general, it is perfectly appropriate to ask whether given types of surveillance are able to achieve their desired objectives. No defender of general government surveillance programs should favour tactics that are counterproductive, or even those that are not cost effective. At the same time, privacy defenders must concede that some surveillance that the government demands is not a waste of time. Therefore, the conflict zone arises over which tactics are effective and which are not. The issues with data collection are not, in principle, different from those that arise with camera surveillances, which have proved invaluable in many instances.

https://doi.org/10.1017/S1574019616000195 Published online by Cambridge University Press

Against this backdrop it was distressing, to say that least, that the views of the Commissioner were categorically rejected when the matter got to the European Court of Justice. At no point in its decision did the Court allude to any of the obvious prudential issues that were in play before the Commission. Instead, the European Court of Justice took the general view that Schrems, or indeed anyone else, could bring to the fore the question of whether the earlier accord was binding so long as an examination of the applicable legal rules showed a gap in the formal level of protection that US law afforded data originating in the EU.

Conceptual jurisprudence and risk management

In making this kind of determination, the European Court of Justice engaged in what is commonly called the jurisprudence of concepts ['*Begriffsjurisprudenz*'][8] or application of the logical method to the study of the law. ['*Grundlage der Begriffsjurisprudenz ist die Anwendung logischer Methoden auf das Recht*.']. In principle, of course, no one should object to the standard task of ordinary language philosophy, which is to correctly characterise the relationship that exists among various concepts of the law. Indeed, one should go further to note that this kind of activity is strictly necessary if legal doctrine is to be able to form such a position. Much of my own work[9] in torts dealing with matters such as causation and assumption of risk are in this tradition: efforts to explain how the traditional legal tools of the American tort law are so muddled conceptually that the tools do not facilitate the clear analysis of basic propositions.

Yet it is equally critical to recognise that the effort to isolate and clarify legal (or indeed any) concepts is only the first stage of the two-stage process. The second stage of this process is to figure how to choose particular remedies and institutional structures to deal with the problems of error and uncertainty that necessarily infect major efforts at regulation. These issues do not come to the fore when the key question is what form of damages should be awarded for completed harms attributable to the conduct of the defendant. In these cases, once the evidentiary record is established, the only issue is to determine how the responsibility for a particular action should be allocated under the various theories of liability.

[8] H-P. Haferkamp, 'Begriffsjurisprudenz/Jurisprudence of Concepts, Enzyklopädie zur Rechtsphilosophie', <www.enzyklopaedie-rechtsphilosophie.net/component/content/article/19-beitraege/105-jurisprudence-of-concepts>, visited 22 June 2016. *See also* para. 94 of the *Schrems* opinion: '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' (emphasis added): ECJ 6 October 2015, Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*.

[9] R.A. Epstein, 'Toward a General Theory of Tort Law: Strict Liability in Context', 3 *Journal of Tort Law* (2010) p. 6.

But much of the law of tort, and huge portions of the regulatory system, are not concerned with giving the proper legal interpretation to legal concepts. Rather the question is how best to minimise the sum of two types of error: Type I error and Type II error. The first addresses a false positive, acting as if some dangerous condition exists when none is apparent. The second is a false negative, which assumes that the condition is safe when in fact some dangerous condition exists. In our context, Type I error involves an invasion of privacy when there is no need to do so. Type II error involves missing a terrorist threat that causes serious harm in order to protect privacy. As noted earlier, many attach a higher severity to the first type of error than to the second. But the greater the importance of Type II error, the more willing governments should be to reduce its occurrence. If what is sought is to minimise the sum of the two types of error, then at the margin we should be willing to accept a far higher level of false positives than false negatives.

The great danger of the jurisprudence of concepts is that it takes the same type of formal approach used to explicate the content of legal principles and uses it to displace the necessary functional analysis about the relative weight of two forms of error. The former inquiry depends only on a clear appreciation of the nuances of the ordinary language that forms the substrate of legal rules. The second depends on a wide-ranging institutional analysis that seeks to figure out how to minimise these two kinds of error in the face of major uncertainty as to both the sources of error and their possible cures. At this point, it is critical to worry about both *ex ante* and *ex post* attacks on various terrorist activities. *Ex ante* precautions are efforts to track and detect these activities before they occur. *Ex post* precautions are meant to apprehend and punish the perpetrators of the various offences. Clearly using the former techniques are necessarily more intrusive than using the latter. Yet by the same token, the prevention of death, injury and mayhem is surely preferable to punishing offenders afterwards when it is impossible, even with the death penalty on the table, to impose any punishment that is proportionate to the crime. Given the increased probability of terrorist events, two conclusions follow. First, the interest in privacy becomes relatively weaker, and, second, the preference for *ex ante* over *ex post* protection becomes stronger.

Adequate protection?

In light of this framework, it is useful to ask why the European Court of Justice gave such a rigid interpretation of the phrase 'adequate protection.' As a matter of ordinary language, the word 'adequate' carries with it an inescapable level of ambiguity. Within the Anglo-American system, the difficulty in dealing with the term is captured by the difficulty of applying the rule that equitable remedies—such as injunctions before the fact—are only given when legal remedies—such as

punishment for wrongful actions—are inadequate. There is no single litmus test which answers that question, but it is surely part of the overall equation that death has no adequate *ex post* remedy for the deceased, and that persons with serious injuries and psychological scars can never be brought back by compensation to the position that leaves them just as well off as they were before the accident. And it should be taken as a given that the sense of terror and the endless set of security precautions required are always uncompensated losses. Given the magnitude of the losses, and the multiple forms in which they manifest themselves, it is perfectly apparent that the collection of *any* damages from terrorist wrongdoers is always an arduous if not impossible task, especially in a world in which individual terrorists are insolvent and foreign governments are noticeably immune from the collection of any adverse judgment, assuming that one could be gained in the first place. For example, is it likely that the Palestinian Authority and the Palestine Liberation Organization will actually pay the $218.5 million verdict[10] entered against them in New York City some 11 years after the 2004 complaint[11] was filed in connection with the January 2002 attacks? *Ex ante* precautions are key to any successful attack on terrorism.

In light of these manifest difficulties it seems wholly incorrect to read the phrase 'adequate protection' as if it meant a perfect level of protection or even the level of protection that the European Union purports to give to its own citizens from various kinds of government oversight. It was therefore incorrect, in my view, for the European Court of Justice to take the position that the American statutory framework had to offer protection 'essentially equivalent' to that supplied under exacting European standards, which started from the assumption that the privacy right in data—apparently even that which has been previously publicly posted on Facebook—was a fundamental interest deserving the highest protection.

It was, of course, no accident that the European Court of Justice made this cryptic reference: 'Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').'[12] That sign of approval for Snowden deserves the harshest of condemnations, for it is clear that Snowden did more than announce that the United States had engaged in comprehensive tracking of metadata. He also provided valuable sources of information about specific operations to Russia and probably China, which surely have compromised the efforts of the United States and its allies to do the intelligence

[10] N. Hong, 'Jury Finds Palestinian Authority, PLO Liable for Terrorist Attacks in Israel a Decade Ago', <www.wsj.com/articles/jury-finds-palestinian-authority-plo-liable-for-terrorist-attacks-in-israel-a-decade-ago-1424715529?alg=y>, visited 22 June 2016.

[11] SDNY 16 January 2004, No. 04-CV-00397, *Sokolow* v *Palestinian Liberation Organization*.

[12] *Supra* n. 1.

work needed to contain various kinds of terrorist threats. The unexplained one-sentence barb contained in the European Court of Justice opinion shows not only its lack of appreciation of the seriousness of Snowden's misdeeds, but also its utter unwillingness to look at both sides of that most complicated process. That one public remark highlights the European Court of Justice's unwise refusal to look closely at the general agreement by which data passed from the EU to the United States.

What is really needed here is a close examination of how the system works, including at least some appreciation of its advantages and disadvantages. Admittedly, the European Court of Justice is the worst institution imaginable to undertake this task, given its own jurisdictional limitations. But it responded to those in the wrong way, by converting a serious problem of institutional competence into an empty and sterile exercise on the meaning and importance of privacy. What it should have done is to ask some commission or national court that has greater powers to conduct this investigation so that it could then make its own explicit error costs calculations. If there is ever an area in which a per se approach is inappropriate for analysis, this is it.

Surveillance and investigation

The mistakes made in the European Court of Justice's reasoning are evident from the court's failure to understand the key difference in approach that is needed for generalised surveillance on the one hand and the investigation of known conspiracies or hostile acts on the other. Thus the Court concluded that any surveillance in the name of national security cannot be pursued on a 'generalized basis.'[13] What the European Court of Justice thinks is needed for the government to act in defence of national security is some 'objective criterion' 'which [is] specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.'

To these American eyes, the European Court of Justice decision was astonishing in several respects. First, the Court misunderstands the nature of surveillance. It is a mistake to require the same specificity of evidence in a general search that is required for the investigation of some past criminal or terrorist act. Quite simply, the general work of surveillance is looking for evidence of network cooperation before the commission of any criminal or terrorist act, which requires an access to large amount of data. The American response[14] has been to give the government greater leeway in tracking connections, even as it

[13] *Supra* n. 1.

[14] The President's Review Group on Intelligence and Communications Technologies, 'Liberty and Security in a Changing World', <www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>, visited 22 June 2016.

imposes restrictions on listening in to various conversations before adequate connections are established.

Second, the European Court of Justice judgment paid no heed whatsoever to the reliance interest of thousands of companies, some large and some small, in the earlier set of rules. It is one thing for a court to shut down a set of untested protocols because they have the potential to become the source of major abuse. It is quite another to shut them down when there is no evidence of concrete abuse anywhere in the system for the 15 years that those practices have been in effect. Yet the Court attached no weight whatsoever to the massive dislocation that its decision would impose on all the companies subject to its decree.

To be sure, it is always possible that some data have been purloined in some unknown fashion for improper uses. But the sad truth is that threats to the security of personal data are much more likely to come from foreign nations or commercial spies than from the various intelligence agencies, which are governed by far stronger institutional safeguards, say, than the Internal Revenue Service, which for its part has direct access to all the sensitive data that is required of any firm, domestic or foreign, that is required to supply information. These harms extend also to the customers of these companies, many of whom, unlike Mr Schrems, are quite happy with the present system developed under Decision 2000/520.

In making this claim for increased surveillance, it does not follow that either the US or the EU should receive from equipment manufacturers a secret back door into the data transfer systems. The objections that I have to this program are not based on the notion that government access under strict protocol works an unacceptable invasion of privacy. It is on the more limited ground that back doors make the system more vulnerable to hacking from hostile sources who can exploit some gap in the more complex architecture in question. In addition, the back door is likely to drive most parties to use technology sold by firms in other countries that are quite happy to assure their eager customers that no back door entry is possible. The point here is subject to lots of technical debate over what tools should be used to break the unbreakable, and what standards should be used to decide when a warrant should be given to allow the government to gain access to this information, assuming that the technical obstacles can be overcome. But again the key task is error minimisation, not according some special weight to the protection of the privacy interest.

Citizens versus aliens

Right now both the EU and the US have put in place systems that give greater protection to their own citizens than to the citizens of other countries. That conscious decision makes it more difficult to determine the appropriate point

https://doi.org/10.1017/S1574019616000195 Published online by Cambridge University Press

of comparison. Right now the European Court of Justice demands the US afford the same level of protection to EU data that it receives in the EU. Another way to put the question, however, is to ask whether the US gives the same level of protection to citizens of the EU that the EU gives to citizens of the US. By that standard, it becomes far more problematic whether the US program is inadequate in comparison to the EU protection for its citizens. It is just this gap, moreover, that makes the treaty solution attractive. Neither side will sell out its own connections, so that we should expect some parity to be achieved.

But at what level? Under the procedure before the European Court of Justice decision, both sides had the opportunity to engage in some form of institutional arbitrage. The US could ask the EU to help it fill in some gaps on its knowledge base of its own citizens, and the EU could reciprocate by offering the same assistance to the US. One risk of the European Court of Justice decision is that it stops a form of cooperation that might be beneficial in light of the domestic obstacles for the collection of reliable intelligence. Indeed, the right question in all these cases is whether both the EU and the US should level up or level down in affording protection against general tactics for surveillance. In my view, the correct approach may well be to ramp up surveillance, so that each side can engage in higher levels of surveillance on its home front than it currently does. Exactly how much is not clear, but an institutional arrangement that puts foreigners and citizens in the same boat has some major institutional advantages insofar as it relieves all governments of the heavy burden of having to manage separately two large and intertwined data sets. Indeed, notwithstanding the constant reference to the Constitution, both the due process protections and the habeas corpus protections embodied in the United States Constitution extend fundamental protections to all persons, not just to citizens.

On this point, the architecture of the Fourteenth Amendment (widely ignored today) established a two-tier structure. The privileges or immunities clause ('no state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States') contemplates a long list of privileges for citizens which includes at the very least the right to acquire property and engage in all occupations. But the due process clause ('no person shall be deprived of life, liberty or property, without due process of law') extends its protection to a wider class of persons, but gives them fewer protections, most notably against arbitrary arrest and confiscation. In dealing with the use of criminal sanctions, there is no gulf between citizens and aliens, which could be reflected in a unitary standard applying to both groups of persons.

Similarly, Article I, Section 9, Clause 2 states, 'The Privilege of the Writ of Habeas Corpus shall not be suspended, unless when in Cases of Rebellion or Invasion the public Safety may require it.' The language of this provision gives no indication when habeas is normally required, for it only addresses the possibility of

its suspension. But no matter how these difficult questions work out, it looks again as though habeas should be available to aliens on the same terms and conditions that it is available to citizens, which once again points to the strength of the unitary standard that is rejected in both the EU and US.

National security and classical liberalism

In closing, I think that it is important to answer the simple question of whether my relatively hardline approach can be reconciled with my own general classical liberal approach that emphasises the importance of private property and limited government. That position starts, of course, from the fundamental premise that the monopoly power in the hands of the state should be regarded with deep suspicion, such that the presumption should be set against the exercise of state power. That presumption holds good in economic areas, where it is in general a mistake for either the EU or the US to interfere in the operation of competitive markets (which they do with near reckless abandon). But the situation with national security is entirely different because the threat or use of force by anyone violates the core libertarian presumption and triggers the right of self-defence, not only for individuals, but for the nation states whose main function is to protect them against the threat of violence, domestic and foreign. At this point the presumption against government action is sorely tested. Indeed, it is overcome, such that the hard question is just how far a state should use the various weapons at its disposal to protect its citizens. That is never an easy question, for sound policies have to run the gauntlet. They cannot be too weak, lest the enemies of the people prevail. They cannot be too strong, lest they snuff out the liberties at home. Getting the right balance is tricky, and one can quarrel endlessly over the correct approach. But the one unacceptable approach is that of the European Court of Justice, which washed its hands of the entire problem by its dogmatic protection of the right of privacy in the face of external threats to bodily and physical integrity. Starting from its dubious premises, the European Court of Justice has ripped apart a system that will take a great deal of effort to put back together, without any showing of an immediate need to act. It takes years to put into place successful complex systems of data transmission. It takes only one errant complaint and a dubious decision of the European Court of Justice to rip it all apart.

https://doi.org/10.1017/S1574019616000195 Published online by Cambridge University Press