Schrems v. Commissioner: A Biblical Parable of Judicial Power

verfassungsblog.de/schrems-v-commissioner-a-biblical-parable-of-judicial-power-2/

Russell A. Miller Mi 7 Okt 2015

David v. Goliath

Even before his big win at the Court of Justice of the European Union (CJEU) on Tuesday, Maximillian Schrems' seemingly quixotic campaign against the giants of America's shadowy security-complex and Internet service sector had attracted colorful allusions to the biblical tale of David and Goliath. It's a good story, except that it is too often misconstrued. The lesson is not that the plucky young Israeli shepherd slew the Philistine giant on his own. The story means to teach us that, even for the unassuming little guy, anything is possible with God's help. King Saul expressed his doubts about David's heroic battlefield delusions. "You are not able to go out against this Philistine and fight him," Saul insisted, "you are only a young man, and he has been a warrior from his youth." But David reassured the King that he wouldn't face Goliath alone: "The Lord who rescued me from the paw of the lion and the paw of the bear will rescue me from the hand of this Philistine." What is a King to say to such a thing, except "Go, and the Lord be with you." As we all know, David went and God was with him. The boy's simple sling and stone brought down the warrior giant.

And so it is that—at least with respect to data privacy—all things are possible if the Luxembourg Court is at your side. We might celebrate the Court's decision in Case C-362/14 as an improbable victory of good (data-privacy) over evil (consumer and intelligence data abuses). But I want to offer some words of caution about god-like judicial power.

A Narrow Reading

The first point of caution is that the CJEU's judgment might be read more narrowly than the biblical metaphor suggests. The next step need not be as exciting as the destruction of the Philistine army. A less sensational reading of the decision might simply be that the European Commission did sloppy work when it issued Decision 2000/520, in which it concluded that the United States ensures an adequate level of protection for electronic communications data. The Commission's Decision wasn't thorough enough, it didn't apply the correct standard, and it wasn't revised to keep abreast of developments. The consequence of this narrow reading of the judgement would simply be to have the Commission issue a new Decision in which it more effectively establishes its conclusion that the U.S. ensures adequate data protection. Could the Commission do this? I don't think so. It is simply the case that the U.S. Constitution's Fourth Amendment and the Foreign Intelligence Surveillance Act extend almost no protection to non-U.S. persons against the intelligence gathering activities revealed by Snowden.

In the Court's pithy reasoning I see only a slender possibility for a new, more palatable Decision from the Commission. In paragraph 91 of the judgment, when articulating the fundamental rights protection guaranteed by Articles 7 and 8 of the Charter, the Court explains that effective data protection includes the assurance (i) that data is protected against abuses; (ii) that data is not subject to automatic processing; and (iii) that there is not a significant risk of unlawful access to data. On these three elements alone, the adequacy of American data protection might still be an open issue. For example, there is the question whether American intelligence community's access to and processing of transferred European data—without additional and more menacing subsequent state action—counts as an "abuse." This possible argument builds on the insights of Ralf Poscher who has suggested that data privacy is better understood as supplementary to more substantive liberty interests. In this view, the collection and processing of data becomes relevant—that is, it counts as an "abuse"—only when it contributes in some way to the state's infringement of other liberty protections, such as the right to free speech or the prohibition on torture. Absent evidence of these additional, more ominous steps, the Americans' access to and processing of European data might not be an abuse. It would also be possible to argue

that the American intelligence community's access to and processing of transferred European data has been achieved lawfully. Those activities are conducted in conformity with constitutional (Fourth Amendment) and statutory (FISA) and regulatory (PPD-28) law. A U.S. federal court decision finding that the NSA's activities exceeded these bounds involved departures from the legal limits placed on surveillance of U.S. persons and not the non-U.S. persons in Europe. It is possible that the new USA FREEDOM Act has remedied these deficiencies in any case. In no case does it appear that American authorities acted unlawfully—that is, outside the scope of the relevant (and admittedly permissive) domestic legal regime—when accessing European data. Nothing about this straightforward assessment is changed by the fact that this legal regime simply does not offer protection to the liberty interests of non-U.S. persons. That, alone, does not make the American intelligence activities unlawful—let alone lawless.

Judicial Restraint

The second point of caution asks whether we really want the CJEU playing God in these matters. If we are determined to have the rule of law apply to a state's intelligence gathering activities (and I think the very concept of clandestine state authority begs this question), then it is not at all clear to me that we mean the kind of Rawlsian, judicially-enforced rule of law the CJEU has secured for itself in its recent string of data-protection cases. In terms that echo Chief Justice Marshall's opinion in *Marbury v. Madison*, the CJEU explains that it "alone has jurisdiction to declare that an EU act … is invalid." (Paragraph 61). But in matters of national security, the U.S. Supreme Court has recognized a different kind of rule of law, one that obliges the unelected judiciary to exercise modesty and restraint in favor of the limitation of government power that can be achieved through political processes, separation of powers, and democratic accountability. This approach—I would call it the "politically enforced rule of law"—is foreclosed by the CJEU's aggressive insistence on its role here. The Commission, whose Decision the Court maligns, is politically accountable to and legitimated by the directly elected European Parliament. The Court, impatient with the slow pace of the European political response to the NSA Affair, is not. It is an old staple of America's quirky anxiety about the anti-majoritarian implications of the judicial role to quote Judge Learned Hand, who wrote "for myself it would be most irksome to be ruled by a bevy of Platonic Guardians, even if I knew how to choose them, which I assuredly do not." That wisdom might be especially resonant for the European Union with its still-fragile democratic legitimacy.

There is more here to recommend the "political enforcement of the rule of law" than just abstract doubts about judicial power based in democratic theory. After all, this issue involves a polity's existential interest in the balance that must be struck between security and liberty. The Court avoids this momentous framing of the case largely by mischaracterizing the interests that it must weigh. At paragraph 42 the Court tells us the dispute requires it to balance the human interest in privacy with the (mostly commercial?) interest in the free movement of data. That might be formalistically true. And if it is, then a result favoring privacy is almost undeniable. Yet, if *sub silentio* the NSA's intrusive programs serve as a moralizing backdrop to the Court's reasoning, then the legitimate and justifiable security motivations for those programs shouldn't be swept off one side of the scale leaving only the anemic commercial interest in the free-flow of data. Privacy or Facebook's hugely profitable commercial model – that might seem to be an easy question. Privacy and access to the data needed to protect against terrorist threats – that's another question altogether. The Court flirts with recognizing America's important security interest in accessing and processing Europeans' data, but it finds that cause more troubling than meaningful. (Paragraphs 84-85). The hard reality of the case, however, is that the Court was deciding between security needs and privacy. Considering the potential consequences of the manner in which that balance is struck, the Court would have been wise to leave these matters in the hands of more accountable and popularly legitimate institutions.

The wisdom of judicial restraint in this context is amplified by the fact that the polity on whose behalf the Court acts itself lacks a sovereign national security mandate. The Union's Common Security and Defense Policy is a strictly inter-governmental affair and, as the German Constitutional Court concluded in its 2009 *Lisbon Treaty Case*, security remains the exclusive interest of the Member States as part of their residual national sovereignty. No EU organ—let alone the cloistered CJEU—is going to have to answer for security threats or lapses in the very tangible and politically-charged way that national institutions and governments will. Doubly insulated in this way, like the smallest piece in a set of Russian nesting dolls, the Court reaches the decision to down-play the

security facets of the case without having to worry about the next terrorist attack. The Court should have taken its artificially sheltered posture into account and deferred to the "political enforcement of the rule of law."

The Role of Courts

The third point of caution begins with the acknowledgement that the proposed "politically enforced rule of law" will sound heretical to European ears that are now well tuned to judicial power, particularly the sweeping power of the courts in Karlsruhe, Starsbourg and Luxembourg. But this preference for political over judicial organs is exactly the approach nearly every country has taken with respect to oversight and control of intelligence services—including their collection and use of telecommunications data. Almost no one submits these questions to ordinary judicial review. Nearly no courts romp about in this field in the way that the CJEU has. The German G10 Act is a compelling case-in-point. It regulates the German intelligence services' constitutionally permissible intrusion on telecommunications privacy. Requested by the intelligence agencies and ordered by the relevant minster, telecommunications surveillance and data-gathering operations must ultimately be approved by the four-person G10 Commission. The G10 Commission definitively is *not* a court. Article 10 of the Basic Law calls it an "auxiliary agency" of the parliament. The commissioners are not judges in the German judiciary. The G10 Act, while establishing the G10 Commission's review, explicitly precludes the German courts from any role in authorizing or monitoring intelligence surveillance operations (at least until after their surveillance objectives have been fulfilled and the need for secrecy has ended). In 1970 the German Constitutional Court confirmed that the G10 Commission is not a judicial organ. The Court was reassured, however, that the G10 Commission's authorization of intelligence surveillance adequately approximated judicial scrutiny. The German regime—and many others like it—recognize what the CJEU, compelled by its self-aggrandizing and federalist impulses, dare not admit: these are areas in which the judiciary should tread lightly, if it must wander in these parts at all.

It will surprise many Europeans to learn that, at least when compared to a judicially-neutered oversight regime such as the one established by German G10 Act, the American oversight framework shows somewhat less skepticism towards a judicial role in these matters. The Foreign Intelligence Surveillance Court (FISC), which also has the responsibility for authorizing and monitoring intelligence community surveillance operations, is a proper federal court staffed by sitting federal judges. With the reforms achieved by the USA FREEDOM Act, the FISC will look and act even more like a court. Its proceedings will be more adversarial and it decisions will be more transparent. But this laudable fact distracts from my broader point, which is that the security issues involved in Schrem's data privacy case should have counseled the CJEU to exercise restraint in favor of the "politically enforced rule of law." In fact, America's experience with these issues—spanning the last forty years—has been that the political and democratically accountable organs can effectively limit and control the intelligence community's excesses. That is the deeply resonant lesson of the Church Committee from the 1970s. Post-Snowden reforms, such as the Presidential Policy Directive 28 and the USA FREEDOM Act, once again justify Americans' confidence in the "politically enforced rule of law."

The Prerogative of Kings – The Power of God

David of course would, himself, become King. Except for occasional, all-too-human failings, he continued to honor God, just as God continued to exalt him. Of course, David's reign and legacy were almost undone by his son Absalom's patricidal campaign and the resulting civil war. David was only able to avoid the seemingly imminent destruction of his kingdom—and his own death—with the help of covert sabotage and the intelligence his spies passed on to him from inside Absalom's camp. God didn't seem to object to this data-collection. But the Court of Justice of the European Union would.

SUGGESTED CITATION Miller, Russell A.: *Schrems v. Commissioner: A Biblical Parable of Judicial Power, VerfBlog,* 2015/10/07, http://verfassungsblog.de/schrems-v-commissioner-a-biblical-parable-of-judicial-power-2/.