

FEATURE

Max Schrems' European Court of Justice Odyssey: Standing up for privacy rights

How one privacy activist took on Facebook, the European Commission, and the United States to protect the rights of European citizens, and prevailed.

By Mihir Kshirsagar and Ross Teixeira

DOI: 10.1145/3437113

On June 25, 2013, Maximillian Schrems, an Austrian privacy activist, filed a complaint with the Irish Data Protection regulator, asserting Facebook Ireland (the operating entity for Facebook in Europe) transferred his personal data to the United States and kept it on American servers, in violation of the European data protection laws [1]. Schrems' complaint sparked a multi-year odyssey to protect the rights of European citizens that set international law ablaze. Schrems won not one, but two, European Court of Justice battles that undid decades of long, complex negotiations involving the flow of data from Europe to the United States (U.S.) and back. Schrems' fight exposed how U.S. privacy law trails European Union (EU) law by kilometers, and how the U.S must catch up sooner than expected.

Schrems' played an "agent of change" in a classic David versus Goliath tale. The issue concerned whether U.S. law could provide adequate protections for EU citizens' data. Schrems didn't think it did, and mounted a zealous legal challenge to overturn the compromise struck between the European Commission and the U.S.

Since the turn of the century, Europe and the U.S have hammered out a set of complex arrangements that govern data sharing between the two continents. The

first version, "Safe Harbor," lasted from 2000 until 2015, when the European Court of Justice struck it down in a challenge brought by Schrems. Their second try, "Privacy Shield," was enacted the following year. It too fell on July 16 of this year, thanks to Schrems' challenge.

The parties are now engaged in a third attempt to find a negotiated resolution. But thanks to Schrems' advocacy, any resolution would likely involve changes in U.S. law to satisfy European concerns, if the third time is to be the charm^[2].

CONTRASTING APPROACHES TO PROTECTING PRIVACY

Policymakers have debated how to protect the privacy of user information since the early days of the commercial internet. One approach, taken by the U.S., allows companies to set their own rules for guarding the privacy of users' information, as long as they disclose these rules to users in privacy policies. But this hands-off policy raises a host of questions: Are privacy policies actually readable by the common user without a legal background or hours of free time? Can users exercise meaningful choice over how their data is used and shared? How are privacy policies enforced? How can a self-regulatory model succeed? Would direct government regulation and enforcement be more effective?



Equally important are the implications for government surveillance within the American self-regulatory approach. How might intelligence agencies exploit the data collected by commercial entities? How can individuals protect their rights against intrusion by public authorities?

In contrast, the EU closely regulates the practices of companies by specifying what they can and cannot do with user data, and provides a mechanism for governments to oversee any disputes about whether a company is taking appropriate action to protect user rights. This tougher approach empowers government agencies to supervise the data practices of large companies, and to keep pace with the newest developments in tech and data sharing. Most of all, it upholds privacy as a fundamental right of EU citizens.

SELF-REGULATION AND COMMERCE IN THE U.S.

In 1997, the Clinton administration's Framework for Global Electronic Commerce

emphasized that securing consumer privacy was essential for the growth of electronic commerce [3]. At the time, survey upon survey showed users were reluctant to provide information without adequate protection for their personal data; the Clinton administration recognized it must act to alleviate this concern. At the same time, the administration was concerned about balancing the "privacy rights of individuals" against "the benefits associated with the free flow of information" to support a thriving market for electronic commerce. In the end, the administration elected to support "private sector efforts... to implement meaningful, consumer-friendly, self-regulatory privacy regimes." But it warned companies that "if privacy concerns are not addressed by industry through self-regulation and technology, the [a]dministration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online."

The self-regulatory model the U.S. settled on was based on voluntary privacy policies and enforcement by the Federal Trade Commission (FTC) for any violations of those policies. Requirements for the content of those policies were left deliberately vague, and described just two fundamental properties: awareness (notice) and choice. Specifically, "Datagatherers should inform consumers what information they are collecting, and how they intend to use such data; and Data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information." This way, users would be empowered to "make better judgments about the levels of privacy available and their willingness to participate." The FTC's enforcement actions, which typically result in settlements where the target company agrees to reform its practices, were designed to create informal guidelines about how other companies might draft better privacy policies.

Very quickly, significant loopholes in the self-regulatory approach became apparent. In 1998, lawmakers had to take action to protect children's privacy rights when an FTC report highlighted that industry had failed to craft an adequate solution. Congress promptly passed COPPA that year to regulate the collection and use of information of websites directed at children under 13 years of age, by requiring companies to disclose their data practices and seek opt-in consent from parents before using any information.

Around the same time in 1998, fearing that Congress would extend the FTC's authority to regulate privacy practices of more websites, the Online Privacy Alliance,

a consortium of companies with significant online presence, agreed on a set of voluntary guidelines to publish privacy policies and self-enforcement mechanisms. The industry group championed data sharing as the default, while offering the consumers the right to opt out of sharing. By aggressively lobbying U.S. policymakers, the Alliance persuaded the government to back off from introducing comprehensive privacy legislation, and to give self-regulation a chance.

The industry's "notice and choice" regime has come to dominate the privacy landscape in the U.S. This approach has left consumers with vague and general statements about companies' data protection practices, combined with a take-it-or-leave-it choice for consumers to agree to the information sharing or lose access to services.

EU: PRIVACY AS A RIGHT

Across the Atlantic, Europe has steered consistently toward greater government oversight of data management practices, stemming from its belief that data privacy is a fundamental right of all citizens. In 1998, just as the U.S. was settling on self-regulation, the EU's Data Protection Directive went into effect. This law required member countries to establish comprehensive privacy regimes that gave EU citizens broad optout rights of data collection, as well as specific protections to control sensitive data, including information about an individual's religious beliefs, sexual orientation, medical history, and financial circumstances. These rights were enforced through designated data protection authorities in member countries.

For data that was collected through websites operating outside Europe, the European Commission entered a series of "Safe Harbor" agreements that aimed to offer EU citizens an equivalent degree of protection to websites based in Europe. Such an agreement was reached with the U.S. in 2000, which allowed U.S. companies doing business in Europe to sell or transfer personal data on EU citizens. The European Commission agreed to accept a compromise position, that the American combination of self-regulation through voluntary disclosures in privacy policies, along with FTC enforcement for failures to adhere to those policies, were equivalent to the EU's comprehensive privacy regulatory system. In return, U.S. companies had to adhere to Safe Harbor Privacy Principles that paralleled EU law. In

addition to notice and choice principles, Safe Harbor allowed EU citizens to access, amend, or delete information; it required U.S. companies to take reasonable precautions to protect personal information; and it provided effective mechanisms for private and public enforcement of compliance with the Principles.

In 2015, the European Court of Justice invalidated the Safe Harbor agreement with the U.S. because there was no mechanism to oversee how intelligence agencies were accessing data as the EU required (stay tuned) [4]. This was a massive blow to the original compromise, but a powerful stance on data protection from the EU.

Schrems' odyssey proves that an individual actor can
force institutions to examine their privacy practices and
stay true to their commitments.

Meanwhile, the EU was overhauling its own approach to protecting privacy. In 2016, it passed the General Data Protection Regulation (GDPR) that protected data collected about European citizens anywhere in the world. The GDPR builds on the 1998 Data Protection Directive and vastly expands the scope of enforcement authority, enough that some academics have called it the "most consequential regulatory development in information policy in a generation" [5]. The GDPR enshrines baseline privacy standards for companies that handle EU citizens' data to adhere to, and provides specific mechanisms for EU citizens to seek redress (appeal) if they believe their rights are not being respected.

Following the collapse of the Safe Harbor arrangement, and in the wake of GDPR, the European Commission took a second shot at a privacy agreement with the U.S. The EU-U.S. Privacy Shield Framework, enacted in 2016, aimed to enable data transfers to U.S.-based businesses that were now no longer permitted under the unlawful Safe Harbor arrangement. To join the Privacy Shield Framework, a U.S. company needed to self-certify and publicly commit to comply with the Framework's requirements. Once it voluntarily committed, those commitments became enforceable under the law by the FTC and state authorities. At least, until Schrems entered the fray.

SCHREMS I: THE PHANTOM SURVEILLANCE

Schrems' journey began in the Spring of 2011 with a class assignment in a seminar on privacy law he took as an Austrian visiting student at Santa Clara University in California [6]. In researching how social media companies collect data on users, Schrems discovered, to his delight, that EU law required Facebook to send Schrems all the personal data Facebook had collected on him. He began a public campaign to unveil the full scope of information Facebook collected on users, and urged other Europeans to request their own data. Just then, a bombshell story hit worldwide press—Edward Snowden, a former U.S. government contractor, exposed the extent to which U.S. intelligence agencies were mining the same information collected by Facebook and other social media companies [7].



Alarmed, Schrems filed a complaint with the Irish Data Protection Commissioner in 2013, alleging Facebook transferred his data to the U.S. in violation of EU law. Schrems' complaint was motivated by Snowden's revelations that U.S. intelligence services, particularly the National Security Agency (NSA), were conducting widespread surveillance of social media activity in U.S. companies. Schrems asserted the law and practice in force in the U.S. did not ensure adequate protection of the personal data of European citizens against the surveillance activities of public

authorities.

The Irish Data Protection Commissioner initially dismissed Schrems' complaint. The Commissioner concluded there was no evidence that his personal data had been accessed by the NSA. The Commissioner added Schrems' complaint was, in reality, a challenge to the Safe Harbor regime, by which the European Commission held that the United States ensured an adequate level of protection for data. As a result, the Commissioner ruled Schrems lacked the ability to question that decision.

Schrems did not back down, and appealed the Commissioner's ruling. At the Irish High Court, he found a more sympathetic audience that was concerned about leaving European citizens with no opportunity to challenge potential violations of their fundamental rights. The High Court focused on the lack of public oversight of the U.S. intelligence services' surveillance of communications, highlighted by the Snowden revelations. The High Court further observed Schrems did in fact challenge the legality of the Safe Harbor regime, and had a right to bring that challenge. The High Court struck down the Safe Harbor arrangement.

The European Court of Justice took a final appeal of the case, and on October 6, 2015, the Court ruled in favor of Schrems. The Court reasoned while the U.S. cannot be required to ensure a level of protection for fundamental rights and freedoms identical to that guaranteed in the EU, it did have to ensure a level of protection essentially equivalent to that guaranteed within the EU. In doing so, the Court emphasized the importance of the U.S. providing effective supervision to detect whether U.S. institutions violate the privacy rights of European citizens.

The Court rejected the argument that the FTC's supervision of privacy policies was sufficient to protect European citizens. First, it observed the FTC's powers were limited to commercial disputes, and "cannot be applied in disputes relating to the legality of interference with fundamental rights...originating from the State." Next, it noted—as suggested by the Snowden revelations—U.S. authorities were able to access the personal data of Europeans and process it in a way that was incompatible with the original purposes behind the data transfer, and beyond what was strictly necessary for protecting national security. Finally, the Court found that European citizens had no administrative or judicial means of appeal in the U.S. that would, for example, allow them to review data the authorities collected on them to

determine if it should be corrected or deleted. As a result, the Court invalidated the Safe Harbor arrangement.

SCHREMS II : ATTACK OF THE CLONE [REGULATION]

In 2015, the European Union and the United States negotiated a new data transfer agreement dubbed the "Privacy Shield," that was ostensibly designed to fix the problems in Safe Harbor. This time, the U.S. government committed to create a new oversight mechanism to protect the rights of EU citizens. This entity, the Privacy Shield Ombudsperson, was placed within the State Department to be (supposedly) independent from U.S. intelligence agencies. The U.S. government also reiterated its commitment to safeguarding EU data against wrongful collection by law enforcement and other government agencies.

Unsatisfied, Schrems filed another complaint against Facebook with the Irish Commissioner ("Schrems II") on December 1, 2015. In this complaint, Schrems argued the new Privacy Shield did nothing to address the problem the Court of Justice had identified with the Safe Harbor arrangement: His data could still be accessed by intelligence agencies in the U.S. without adequate oversight. Therefore, he petitioned the Commissioner to once again prohibit the transfer of his personal data on Facebook to the U.S.

On May 24, 2016, the Irish Commissioner, this time agreeing with Schrems, published a provisional view that the personal data of EU citizens transferred to the U.S. did not have the equivalent protections that were available in the EU. The Irish High Court upheld that view. In particular, the court noted Section 702 of the U.S. Foreign Intelligence Surveillance Act permits bulk surveillance of European citizens (among other targets) as part of surveillance programs, such as PRISM and Upstream, which the Snowden revelations had highlighted. For the PRISM program, internet service providers were required to supply the NSA (and on occasion, the Federal Bureau of Investigations (FBI) and Central Intelligence Agency (CIA)) with all communications to and from a person of interest (called a "selector"). Similarly, for upstream programs, backbone internet providers were required to allow the NSA to copy and filter internet traffic flows, including metadata and the content of communications.

Crucially, the Irish High Court found the Fourth Amendment to the U.S. Constitution, which prevents "unreasonable searches and seizures" of U.S. citizens' data, does not give EU citizens the right to challenge unlawful surveillance. The High Court also found U.S. law makes it exceedingly difficult for European citizens to bring legal challenges in U.S. courts against government action. Finally, the High Court viewed the new Privacy Shield Ombudsperson as an insufficient check on intelligence agencies as the position resided within the executive branch, under control of the President, and thus could not be a truly independent tribunal.

The European Commission challenged Schrems to a final showdown to save Privacy Shield. On appeal, the European Court of Justice quickly disposed of the Commission's first objection: that Schrems had given Facebook his consent to transfer data to the United States by accepting Facebook's privacy policy. The Court also confirmed its requirement from its Safe Harbor decision that the U.S. had to ensure an essentially equivalent protection for fundamental rights and freedoms to those guaranteed within the EU. It then proceeded to assess if the Privacy Shield arrangement offered that level of protection.

The Court's analysis focused on the Privacy Shield "Principles" clause that allowed data to be accessed or used "to the extent necessary to meet national security, public interest, or law enforcement requirements." The Court noted the interception of personal data by an intelligence agency constitutes an interference with the fundamental rights enshrined in EU law. To allow interference with those rights, the Court reasoned, there must clear and precise rules about the circumstances and conditions for when data is intercepted, and a mechanism for users to pursue legal remedies.

The Court noted that the U.S. government had itself conceded in its submission to the Court that European citizens had no actionable rights before the courts against U.S. authorities. In addition, there is no U.S. law that gives a European citizen the fundamental right to review personal data relating to him or her, and have the opportunity to correct or delete such data; nor did the Ombudsperson provide this remedy. As a result, the Court struck down the Privacy Shield arrangement. Schrems and EU citizens - 2, EU and U.S. authorities - 0.

SCHREMS III: REVENGE OF THE COMMISSION?

Efforts are now underway to replace the Privacy Shield arrangement with a more robust mechanism under U.S. law, to give European citizens the fundamental data protection rights guaranteed to them under EU law. At the same time, Schrems' actions have emboldened activists in the United States in their demands for similar rights against unchecked government surveillance. If the U.S. is willing to extend protections to European citizens to review and challenge the data about themselves collected by intelligence agencies, surely American citizens should be offered the same protections?

Schrems' odyssey proves that an individual actor can force institutions to examine their privacy practices and stay true to their commitments, upending decades of international law in the process. The journey is long and arduous, but history rewards the righteous.

Biographies

Mihir Kshirsagar runs an interdisciplinary technology policy clinic at Princeton's Center for Information Technology Policy. Before joining the academy, he was a litigator with experience in private practice and public service. He graduated from Harvard and has a law degree from the University of Pennsylvania.

Ross Teixeira is a second-year Ph.D. student at Princeton's Center for Information Technology Policy, and a Siebel Scholar. His work measures internet infrastructure to answer pressing public policy questions intersecting society and the internet, with an emphasis on privacy, access, and bias against marginalized groups.

Copyright is held by the owner/author(s).

Publication rights licensed to ACM.

1528-4972/20/12 \$15.00

References

[1] Court of Justice of the European Union. Judgment of the Court - 6 October 2015 Schrems Case

C-362/14 ECLI:EU:C:2015:650 2015