Adequacy of data protection in the USA: myths and facts

Lothar Determann*

On 6 October 2015, the European Court of Justice (CJEU) invalidated a decision from 2000, wherein the Commission had granted an exception from the general prohibition regarding transfers of personal data outside the European Economic Area (EEA) (CJEU C-362/14, Schrems v Data Protection Commissioner 6 October 2015). Companies in the EEA were permitted to transfer personal data to US companies that had registered under the US Safe Harbor programme (Commission Decision 2000/520/EC, OJ L 215, 25 August 2000, 7). Data protection authorities in all EEA Member States retained their authority to suspend data transfers in case of concerns regarding the level of data protection in the USA, but never exercised this power, not even after Edward Snowden’s revelations in 2013. The CJEU judgment responded to questions from an Irish court regarding the dismissal of a complaint by the Irish Data Protection Commissioner who did not share the complainant’s concerns regarding the level of data protection in the USA. After the CJEU judgment, a number of myths started to establish themselves, including the following (for more details on the sources of myths and facts, see Determann, U.S. Privacy Safe Harbor—More Myths and Facts, Bloomberg BNA Privacy & Security Law Report, 14 PVLR 2017 (2015)):

- The CJEU had adequately examined the level of data protection in the USA; however, there are no indications for any such examination in the court’s opinion.
- The CJEU had terminated a Safe Harbor agreement or treaty; but there never was a binding agreement—only the programme, unilaterally implemented by the US Department of Commerce and the—now invalidated—unilateral decision by the Commission according to which the Safe Harbor programme contributes to a level of data protection that is adequate from the European perspective.
- The CJEU had invalidated the Safe Harbor programme; yet, the programme is not subject to the jurisdiction of the CJEU and has been continued by the US Department of Commerce for now.
- The roughly 5500 US companies in the Safe Harbor programme had been seriously affected by the CJEU judgment; however, the CJEU judgment concerns directly only European companies, probably in much greater numbers, which suddenly had to justify their data transfers to the USA differently; in this regard, the European companies can choose between a number of alternatives, which require time and bureaucratic efforts; actual changes in data transfer practices are not apparent to date.
- The CJEU decision had increased the level of data protection for Europeans; yet, the immediate effect of the CJEU judgment was a reduction in protection for European data in the USA, because the CJEU damaged an institute of cooperation and interoperability with which the US government had enforced EU data protection law principles on US territory.
- The Safe Harbor programme had not been effective, because it only required self-certification; however, a formal self-certification of a corporate officer in the USA is quite an effective mechanism, given the strict sanctions threatened by US laws, and many EU Member States, including Germany, do not contemplate any certifications by local authorities or third parties, not even a self-certifications as the CE-marking regime requires for products.

Facts

The Commission had conducted a detailed examination regarding the question whether the level of data protection in the USA is adequate in the year 2000. It had concerns in this respect and limited the exception from the general prohibition of data transfers outside the EEA concerning the USA to companies that committed in a legally binding manner to the Safe Harbor Principles,
which were in turn framed based on principles of EU data protection law. This limitation is unique and noteworthy. In other decisions, the Commission decided without limitations that the level of data protection was adequate, for example, in Argentina, Canada, Israel, and New Zealand, even though these countries are not generally known to have particularly strict data protection standards, particularly not regarding the regulation of secret service activities (see, for example, Tene, Systematic Government Access to Private Sector Data in Israel, 2 International Data Privacy Law 277, 279ff (2012); for Commission Decisions, see <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 16 February 2016).

At the time when the CJEU cast its judgment, about 5500 of roughly 6 million companies in the USA had registered under the Safe Harbor programme and thus committed to compliance with EU data protection law principles. Most companies in the USA are processing some personal data from Europe. US companies can hardly avoid processing personal data from Europe, because trade connections with Europe are strong and any routine business communications with European companies necessitate processing of personal data, given the broad definitions of ‘personal data’ and ‘processing’ under EU laws. According to EU data protection law, any information relating to an identifiable person constitutes ‘personal data’ (Data Protection Directive 95/46/EC, Art 2(a) (hereinafter ‘Data Protection Directive’)), including the name and office phone number of the employee of a European company that wants to sell cars or order computers in the USA. To answer the question whether the level of data protection in the USA is higher, lower, or equivalent compared to the level in the EEA, Argentina, Canada, Israel, or New Zealand, one has to first understand, assess, and compare data protection laws, data processing practices and actual conditions of individual privacy and information self-determination in the different jurisdictions. The CJEU did not address these topics in any depth but merely referred to the vague assertions of the complainant in the Irish proceedings as well as media reports about National Security Agency (NSA) espionage, without establishing a comparative context to media reports about quite similar surveillance activities of the secret services in the EEA.

Analysis

Differences in data protection laws in the USA and the EEA

Compliance and enforcement

Government authorities and private plaintiffs enforce US laws quite rigorously, with heavy fines and damages, often reaching millions in the context of class action lawsuits, particularly in the area of data protection laws (the terms ‘data privacy’ and ‘data protection’ are often—and in this article—used interchangeably in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws, even though the two terms and legislative concepts have quite different origins and purposes. For more detail on this point, see Lothar Determann, Determann’s Field Guide to Privacy Law (2nd edn., 2015, Edward Elgar Publishing, London, UK); Lothar Determann, California Privacy Law (2015, The Recorder, San Francisco, California, USA). In continental Europe, on the other hand, data protection laws have a 45-year history and always contemplated damages, fines, and even imprisonment. But, in practice there are only a few and only recent examples of actual enforcement of data protection laws in Europe.

For example, only in the year 2015, the Bavarian data protection authority made headlines by taking action against the common practice of companies to transfer customer data as an asset in the context of mergers and acquisitions, by issuing a fine to ‘state an example’(see <www.datenschutzbeauftragter-info.de/kundendaten-datenschutzrecht-beim-unternehmenskauf/> accessed 16 February 2016). In the USA, the Federal Trade Commission had tackled this issue already fifteen years earlier (see <www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc> accessed 16 February 2016). Also, under EU data protection laws, companies always needed express consent from Internet users before they could lawfully collect personal data via web cookies, because any processing of personal data without consent or other justification was prohibited. Nevertheless, Internet users can easily testify that European companies did not comply with such general prohibitions under national data protection laws from the seventies, nor with ‘opt-out’ requirements introduced by EU law in 2002, nor with the ‘opt-in’ consent requirement re-introduced by EU law in 2009 (Data Protection Directive Arts 2(h) and 5(3) Directive 2002/58/EG; Determann, ‘How to Ask for a Cookie: Information Technology, Data Privacy and Property Law Considerations’ (2010) 15 BNA Electronic Commerce Law Report 8). The same web cookie technologies were and are used in Europe and in the USA. According to US law, adequate notice and implied consent have been sufficient. Notice and implied consent is also what companies and government agencies—including many European data protection authorities—seem to be relying on with respect to the use of cookies on their own websites. But, enforcement actions against misleading disclosures and ineffective opt-out
mechanisms regarding cookies have been brought systematically only in the USA.

Specificity, concreteness, detail

Individuals are protected by US privacy laws in a differentiated manner based on risk considerations with respect to privacy, informational self-determination and freedom of information. Hundreds of sector-, industry-, and risk-specific consumer protection and data protection laws, at the federal and state level, address threats and balance conflicting interests, including freedom of speech, technological progress, and private enterprise (see Solove and Schwartz, Information Privacy Law (6th edn 2015, Walters Kluwer, Alphen aan den Rijn, the Netherlands); Determann, California Privacy Law (2016, American Lawyer Media and The Recorder, San Francisco, California)). Lawmakers can influence business conduct and consumer protection more effectively with the sector specific prohibitions and limitations under US law than with the general prohibition of any automatic processing of any personal data under EU law. Wherever everything is generally prohibited, in practice, exceptions are claimed generally too. As a consequence, the true limitations of applicable law remain unclear and unable to safeguard effective protection.

The case that ultimately resulted in the CJEU judgment of 6 October 2015 illustrates this quite well: the case started with a complaint of an Austrian who had used a social network voluntarily and free of charge since 2008 to disseminate information about himself via the Internet. Social networks are not primarily intended for secret communications but for the distribution of personal information, which private individuals compile in their own discretion for private purposes and provide to more or less carefully selected friends in accordance with terms of use of the network operators. Operators fund their social network offerings by selling space for advertising to companies, which try to customize the ads based on interests of the individual users to be effective. Social network operators usually place servers in different countries and continents to optimize access and availability for users, minimize latency, protect against natural catastrophes and cyberattacks and establish ‘follow the sun’ support, 24 × 7 × 365. This does not adversely affect data privacy interests of network users. The networks are intended to globally connect users across national borders. One single global network, available worldwide, serves the interests of users in social networking best and requires international data transfers by necessity. Data that anyone posts about herself or her friends should or could be forwarded by friends and acquaintances at their discretion anyhow and can always end up in the USA and any other country, regardless of where servers are located. The NSA can access information on social networks via publicly available search engines just as much as secret services in Europe, North Korea, or Syria, regardless whether data is stored on servers that are located in Austria or the USA. In light of this and the lack of any substantiated harm associated with alleged NSA espionage on information disseminated via social networks, US data protection laws and courts would dismiss claims for lack of standing and intrusion into reasonable data privacy expectations. For similar reasons, the Austrian claimant initially failed in his home country: the lower court in Vienna denied him standing under consumer and data protection laws (see <http://wien.orf.at/news/stories/2719001/; reversed on appeal http://wien.orf.at/news/stories/2738050/> accessed 16 February 2016). Equally, and because it was already the 23rd complaint of the claimant who must have been intimately familiar with the data processing practices of social networks by now and continued to use it voluntarily and free of charge, the Irish data protection authority had dismissed his complaint as ‘frivolous and vexatious’. The fact that the Irish High Court and ultimately the CJEU believed that they had to intervene just in a case like this—where the plaintiff can hardly show any plausible harm or need of protection—to issue the first major decisions regarding the 20-year-old prohibition of international data transfers under EU data protection laws is symptomatic for the undifferentiated rigidity of EU data protection law, which, if applied consistently, has to result in unconvincing judgments like the one issued by the CJEU on 6 October 2015. This becomes apparent only now and relatively late in the history of EU data protection laws, because the same have not yet been subjected to reality checks in court much, due to the general lack of enforcement.

Most US data protection laws, on the other hand, are applied relatively quickly by authorities or courts. Therefore, US lawmakers try to frame data privacy laws with much more specificity, concreteness, and detail, to reduce avoidable ambiguities and controversies. Also, they limit prohibitions and claims to situations that affect legitimate privacy expectations. If network operators mislead consumers or change rules without user consent to publish more data than users agreed to or fail to protect confidential information against unauthorized access by thieves and fraudsters, then US data and consumer protection laws apply. Then, US authorities and plaintiffs bring actions—swiftly and with determination (Determann, Social Media @ Work 2014, BNA/Bloomberg Social Media Law & Policy Report, 2 SMLR 49, 17 December 2013). On the other hand, it is unproblematic according to US law if police and secret
services collect data that is published on social networks or if companies exchange contact information of their employees across borders in the interest of international business dealings, because this does not affect reasonable privacy expectations of individuals.

According to currently applicable EU data protection law and in particular the CJEU judgment of 6 October 2015, companies in the EU are immediately prohibited without any transition period from transferring any personal data to the USA, even personal data that individuals publish on social networks, unless other special measures are implemented (eg execution of ‘Standard Contractual Clauses’ promulgated by the EU Commission or ‘Binding Corporate Rules’ approved by national data protection authorities, neither of which can have any impact on data collection practices of the NSA or European secret services). This prohibition applies immediately also with respect to data categories that hardly deserve special protections, for example, the name or office phone number of a sales employee who is tasked with selling European cars in the USA.

Of course, companies in the EEA can still not comply with the general prohibition of international data transfers in EU data protection laws, even after 6 October 2015, as they have been unable to fully comply with many other EU data protection law requirements, which have been too undifferentiated and unspecific from the outset. Residents of the EEA continue to use social networks and other services offered by US companies since 6 October 2015 as they have before. Companies on both sides of the Atlantic continue their good trade relations in mutual interest. Civil and military government authorities continue to cooperate, too. The theoretical requirements of EU data protection law with respect to international data transfers continue to have little impact on the actual level of data protection in the EU.

Up to date

US lawmakers continuously update existing and enact new data protection laws to address risks associated with new technologies and business models. For example, in 2002 California passed the world’s first law to require companies and government agencies to notify data subjects regarding data security breaches. California’s data security breach notification law became effective in 2003 and a model for similar laws in nearly all other States in the USA and many other countries. California has been updating and expanding the law routinely, including protecting additional data categories, such as online account credentials in 2014 and automated license plate recognition system data in 2015. Also, California required online service providers in a 2004 statute to post privacy policies and updated the law in 2014 to require specific disclosures regarding how operators respond to ‘do not track’ signals (California Business & Professions Code s 22575(b)).

EU data protection law on the other hand is based largely on national statutes from the seventies, which were adopted without improvements into the harmonizing Data Protection Directive in 1995, when phenomena like the Internet, email, mobile phones, social networks, digital cameras, and modern information technologies were not yet widely known or considered in the legislative process. Since 1995, the Data Protection Directive has not been updated at all and very few other EU data protection laws were added.

No general prohibition of automated processing of personal data

One crucial difference between US and EU data protection laws is that US lawmakers have not enacted a general prohibition or minimization duty regarding automated processing of personal data. In the EU, companies are generally prohibited from processing personal data, unless they can claim a special statutory exemption. The US Congress considered a similarly broad data protection law in the seventies but decided against it, because it would have obstructed the evolution of information technologies too much, only few concrete risks were apparent, comprehensive regulation at the federal level could have resulted in unreasonable ossification in this field of law and a broadly worded European-style prohibition would have triggered a wave of litigation with catastrophic consequences for freedom information, innovation, and commerce given the general enforcement climate in the USA (Schwartz, ‘Preemption and Privacy’ (2009) 118 Yale Law Review 902).

No data protection bureaucracy

In the USA, consumer protection watchdogs, police, regulators, and general law enforcement authorities enforce data protection laws like other laws. The California Attorney General has created a ‘Privacy Protection and Enforcement Unit’. But there are no special data protection authorities, database registration duties or data processing approval requirements as in the European Union. Instead, data protection law enforcement is additionally ensured by plaintiff-friendly civil procedure law and class actions.

No specific restrictions on international data transfers

The USA support free global trade and have so far not retaliated against the protectionist data transfer
restrictions in ‘Fortress Europe’. UK companies are permitted to transfer personal data relatively freely and without any particular adequacy assessments, into any EEA Member States, including recently admitted Member States as, for example, Romania—but not into the USA. US companies on the other hand just have to comply with US data protection laws—regardless where the data are ultimately processed. US companies are not restricted with respect to data transfers to Europe even though European courts and agencies have so far not offered to enforce US data protection laws, for example, via a reverse Safe Harbor or Privacy Shield programme.

Freedom of speech and information

The US Constitution protects freedom of speech and information in the first amendment with particular rigor as a crucial safeguard for democracy and minority protection. Incompatible with such protections is a general ‘right to be forgotten’, as the CJEU has created, according to which data protection authorities and courts in the EU can force companies to suppress or obscure true and publicly known facts in search results (in the case at hand a statutorily required public foreclosure notice concerning the Spanish lawyer Mario Costeja González) (CJEU, C-131/12, Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 May 2014. See also Determann, ‘Social Media Privacy – 12 Myths and Facts’ (2012) 2012 Stanford Technology Law Review 7). From the US perspective, it would not be acceptable that lawyers or politicians could misuse such rights to manipulate public opinion—a risk that has been illustrated by the immediate adoption of the CJEU creation into Russian law by the Putin regime. In light of specific risks concerning minors California had enacted a much more balanced law in 2014 according to which minors must remain able to withdraw their own posts (California Business & Professions Code s 22581(f)). Determann, Francis and Zee, New California Privacy Laws, BNA Privacy & Security Law Report, 12 PVLR 1820 (2013)). Aside from this, only slander, libel and false light publicity are actionable under US law.

No statutory requirement to appoint data protection officers

Different from Germany, but similar to the UK and most other EEA Member States, the USA do not generally require companies to appoint a data protection officer. Some sector specific laws require appointments, eg Health Insurance Portability and Accountability Act for health care sector companies as well as some public sector laws for government agencies. For example, the NSA has to appoint a data protection officer since 2014, as a reaction to the publicized data privacy and security violations at this agency. Nevertheless, many companies and agencies in the USA have voluntarily appointed ‘Chief Privacy Officers’ and hired or trained in-house counsels specializing in data protection laws to enhance compliance and mitigate risks.

Compelled government access to personal data

According to the 4th Amendment of the US Constitution, US authorities need probable cause and a warrant issued by a court to conduct searches and seizures. The Federal Constitution applies these protections only against state actors and on US territory. Article 1 of the California Constitution, on the other hand, guarantees a civil right to ‘privacy’ also against private companies and individuals pursuant to a proposition by the California people in 1972. Additionally, statutes and courts have extended privacy protections also to foreigners and other intrusions into reasonable privacy expectations, including location data and access to stored emails (see, for example, Warshak v United States, 631 F 3d 266 (6th Cir)).

Regarding the requirement of a court order and probable cause, the legal situation in the EEA Member States is much less stringent or uniform. For example, in some EEA Member States, senior police or military officers can issue search warrants (see Study of the EU Agency for Fundamental Rights (FRA), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States’ legal frameworks (2015) <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services> accessed 16 February 2016: A comparison between USA and EU data protection legislation for law enforcement purposes <www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf> accessed 16 February 2016). The currently applicable Data Protection Directive expressly carves out from its scope national security measures, which raises the question what level of data protection the CJEU meant to compare the situation in the USA to in the context of its comments regarding ‘equivalence’ (it is worth noting that the EU Data Protection Directive 95/46/EC requires ‘equivalence’ only with respect to data protection laws in the EEA Member States, see Art 31.2. With respect to third countries, the Directive requires ‘adequacy’, see Arts 25 and 26, given that it would be unrealistic and counterproductive to demand total worldwide harmonization of data protection laws. The CJEU, however, ignores the prudent distinction in the Directive, see CJEU C-362/14 Schrems v Data Protection...
Differences in data processing practices in the USA and the EU

Due to globalization and economic cooperation between Europe and the USA, the differences in data processing practices in the private and public sector appear relatively minor.

Regarding the private sector, the same providers present the same offerings on both sides of the Atlantic. Social media and online services are largely global and funded through advertising revenue and commercial use of personal data. It is worth noting that most of the leading businesses and information technologies worldwide originate from the USA, for example, in the fields of computers, software, cloud computing, Internet, online services, and social media. One of the reasons seems to be that USA have not generally prohibited the automated processing of personal data and deterred entrepreneurs and investors with overbroad and rigid laws (Chander, ‘How Law Made Silicon Valley’ (2014) 63 Emory Law Journal 639).

Regarding the public sector, it is clear that in both jurisdictions—USA and EU—governments engage in surveillance, violate data protection laws, and cooperate so closely that it seems to hardly matter whether data is stored in Europe or in the USA (Determann and Guttenberg, ‘On War and Peace in Cyberspace: Security, Privacy, Jurisdiction’ (2014) 41 Hastings Constitutional Law Quarterly 1, 7). Edward Snowden’s revelations did not only embarrass the NSA, which ignored applicable US laws and has been enjoined by US courts since 2013 (Klayman v Obama, No 13851, (RJL), 2015 BL 368678 (DDC 9 November 2015)), but also the secret services of numerous EEA Member States and reminded the public that since the Second World War British intelligence agencies have been systematically exchanging information with agencies in the USA, Canada, Australia, and New Zealand as part of the ‘Five Eyes Alliance’. Since EU law prohibits restrictions on the free flow of personal data to the UK, personal data must unavoidably end up in the USA. It appears quite unjust and inadequate that the CJEU fails to acknowledge these unchanged realities of international intelligence cooperation in the context of its adequacy assessment regarding the level of data protection in the USA and burdens private sector cooperation precisely because of concerns regarding government activities when the very government cooperation remains unaffected by the court’s judgment.

Differences in USA and EU privacy conditions from the data subject’s perspective

Individuals have generally more effective privacy rights and claims in the USA than in the EU, as evidenced by the many individual and class action lawsuits in the USA and the relative dearth of such suits in Europe. Civil claims and remedies against US companies are available equally to Americans and Europeans in US courts.

Regarding actual options to protect individual privacy, the author of this article, as a citizen of the USA and the EU, personally and subjectively perceives the situation in both jurisdictions quite similarly. At borders and in public places, citizens are subject to surveillance and increasingly to biometric data capture (Adequate according to EU data protection law: CJEU, C-291/12 (Schwarz v Bochum)). At home, one can choose seclusion or exhibition in social media. At work, US residents are monitored more by employers but in return harassed less by colleagues (Determann and Sprague, ‘Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States’ (2011) 26 Berkeley Technology Law Journal 979). On the German Autobahn and at road intersections with traffic lights, drivers are monitored and photographed more by speed and red light controls than in the USA. There are certainly differences in details, but hardly a compelling case for perceivably lower data protection levels in general. The readers of this article may decide for themselves whether they experienced greater intrusions in their privacy or greater restrictions on their personal right of information self-determination when they last visited the USA.

Regarding the topic of surveillance by intelligence services in particular, it is worth considering that the
perception of citizens in the EU and the USA are framed by different historic experiences. In Europe, people have greater concerns regarding threats from government agencies and bad memories regarding the ‘geheime Staatspolizei’ (Gestapo) of the Third Reich and the ‘Staatssicherheit’ (STASI) of the East German ‘DDR’, which completely disrespected personal privacy until 1990. The NSA is not known to have committed any comparably horrific misdeeds against Americans or Europeans, but at worst been overly ambitious in its attempts to protect the USA and its allies in Europe against international terrorism. The US government took steps against the recent data protection law violations by the NSA in ways that seem adequate from the perspective of the democratically legitimated institutions and apparently also of the majority of the US population. US residents are more concerned regarding the expansion of international terrorism since the attacks of 11 September 2001 in New York City and demand from their government first and foremost effective national security. Since the attacks in Paris on 13 November 2015, the relative preferences between privacy and security seem to be in flux also in Europe. Calls for intensified cooperation with US intelligence services become louder. Regarding airline passenger data monitoring, some EEA Member States are proposing security measures that other EEA Member States have been trying to talk the USA out of since 2001 (see, Determann, ‘Conflicting Data Laws: Airlines Are Damned if They Do, Don’t’ (2003) 8 Cyberspace Lawyer 6; Die USA und Frankreich rücken näher zusammen - Vertiefte Kooperation der Nachrichtendienste, NZZ vom 18 November 2015). In the context of this debate, one should not forget that the USA have made a significant contribution to the protection of national security and human rights in Europe in the last 100 years and most EU and EEA Member States nearly completely rely for their protection on the US military and intelligence. The Irish High Court had expressly acknowledged these realities (High Court of Ireland, Schrems v Data Protection Commissioner [2014] IEHC 310, 2013 765 JR, 18 June 2014, 66, ⟨http://www.bailii.org/ie/cases/IEHC/2014/H310.html⟩ accessed 16 February 2016).

The theoretical requirements of EU data protection law with respect to international data transfers continue to have little impact on the actual level of data protection in the EU. This fact should be considered in light of ongoing negotiations between the USA and the EU on a modified ‘Shield’ privacy arrangement. If better data protection levels is the true objective of updating the Safe Harbor programme, then the EU should consider making the reach of the programme bidirectional and also apply and enforce the more effective, specific and up-to-date US data privacy laws in Europe.