Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

Introduction

Alan Charles Raul
Sidley Austin LLP

practiceguides.chambers.com

2021

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Dynamic Privacy Developments Spur Compliance and Disquiet

In a physical sense, we have all suffered from an undesired degree of too much personal privacy in the last 12 months of COVID-19. And in the digital realm, the world's governments have handed down substantially more data privacy legislation to digest during this same period.

The California Consumer Privacy Act (CCPA) took effect at the beginning of 2020, the new Brazilian data protection law a year later and, most recently, the enactment of another full-on GDPR/CCPA-type law took root in the Commonwealth of Virginia. There is no rest for the weary in the privacy field. And no stability either.

Schrems II

In July 2020, the EU's Court of Justice (CJEU) struck down the US–EU Privacy Shield authorisation for transatlantic personal data flows, and required companies exporting data to the USA to conduct elaborate self-assessments of whether the American national security surveillance law interferes with private companies' ability to comply with their "standard contractual clauses" (SCCs) for data transfers.

Theoretically, the CJEU's decisions in Schrems II requires such assessments of the national laws of every country to which personal data is transferred pursuant to SCCs, but in reality, the CJEU seemed concerned only about the US foreign intelligence surveillance.

The Schrems II opinion suffers from extensive substantive gaps in addressing actual US statutory, administrative and judicial safeguards, checks and balances, and independent oversight governing national security access to foreign data. But most significantly, the Court failed to appreciate that SCC transfers to the USA may not even be lawfully targeted under the section of US law – the Foreign Intelligence Surveillance Act (FISA 702) – that the CJEU was most worried about.

In fact, SCC transfers to the USA are quintessential "US Person" communications that US intelligence agencies are prohibited from targeting under FISA 702. In other words, the primary concerns expressed by the CJEU regarding the National Security Agency's allegedly disproportionate and legally unconstrained surveillance of EU data were simply misplaced. The legal grounds for this view are set forth in detail in my paper for Data Matters (Sidley's cybersecurity, privacy and data protection law blog).

Notwithstanding the CJEU's quixotic mandate, however, every company transferring data to the USA is now required to perform analytic somersaults to justify the American legal system. Prescinding from the double standards at issue, and the fact that SCCs are intended to be used precisely for transfers to countries whose privacy regimes have not yet been found "adequate" by the EU, no company can today feel totally confident its SCCs will hold up against legal challenge – despite that company's very best efforts and intentions to comply with EU law. Thus, without any empirical – or indeed legal – predicate for overturning a previously stable regime for international data transfers, the CJEU has tossed settled understandings of data protection out the window and exposed law-abiding international companies to ineluctable uncertainty.

California privacy legislation

California has done likewise. After two years of working to implement compliance programmes to satisfy the GDPR-emulating CCPA, the state's citizens voted in November 2020 to enact a replacement for CCPA (by citizen plebiscite): the new California Privacy Rights Act (CPRA), which shifts the goal posts once again. Though the CPRA builds on the CCPA, the ever-moving target for privacy compliance is only good for lawyers – a small consolation about which some may be grateful.

The need for federal legislation and transatlantic dialogue

It has come to this: the US Congress and the administration of President Joe Biden must save the day at home and abroad.

To rationalise and stabilise privacy and data protection law, the administration must make two things must happen. First, there must be federal legislation that supersedes the burgeoning babel of conflicting state laws. Compliance with a sound federal privacy law would be both manageable and meaningful. Compliance with a conflicting, ever-changing and unpredictable congeries of state laws is just make-work. And make nervous. Privacy professionals and their corporate leadership deserve to be held accountable to understand intelligible standards, not quantum mechanics. The Heisenberg Uncertainty Principle is simply not an ideal framework to achieve effective data protection.

Second, the USA and EU should immediately re-engage in a transatlantic dialogue on digital trade. There must be mutual recognition of each other's data privacy regimes that is codified in a treaty binding on EU institutions, including the CJEU. This should be eminently doable between two like-minded, privacy-loving, democratic, human-rights-respecting jurisdictions.

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Indeed, it bears recalling that, on 2 June 2016, the USA and EU already acknowledged as much (in the Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses). The parties to this 2016 Agreement agreed as follows:

"… the *United States and the European Union are committed to ensuring a high level of protection of personal information* exchanged in the context of the prevention, investigation, detection, and prosecution of criminal offenses, including terrorism; [intend] to establish a lasting legal framework to facilitate the exchange of information, which is critical to prevent, investigate, detect and prosecute criminal offenses, including terrorism, as a means of *protecting their respective democratic societies and common values*; … [and recognise] that certain existing agreements between the Parties concerning the processing of personal information establish that those *agreements provide an adequate level of data protection* within the scope of those agreements … [and] *both Parties' longstanding traditions of respect for individual privacy* including as reflected in the Principles on Privacy and Personal Data Protection for Law Enforcement Purposes elaborated by the EU-U.S. High Level Contact Group on Information Sharing and Privacy and Personal Data Protection, the Charter of Fundamental Rights of the European Union and applicable EU laws, the United States Constitution and applicable U.S. laws, and the Fair Information Practice Principles of the Organization for Economic Cooperation and Development; and [recognise] *the principles of proportionality and necessity, and relevance and reasonableness, as implemented by the Parties in their respective legal frameworks* …." [emphasis added]

In other words, if the USA and EU could proceed to dispense with double standards, it should be quite easy to accord mutual recognition predicated on each side's: (i) "high level of protection of personal information"; (ii) "common values"; (iii) respective "adequate level of protection"; (iv) "longstanding traditions of respect for individual privacy"; and (v) "the principles of proportionality and necessity, and relevance and reasonableness, as implemented by the Parties in their respective legal frameworks".

The USA must advocate for legally binding mutual recognition of both sides' respective data privacy standards, and the EU must grant it.

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Geneva, Hong Kong, Singapore and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, tech, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, digital governance, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as GDPR and CCPA; legislative and policy developments; and international data transfers.

Contributing Editor

Alan Charles Raul is a partner and the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on federal, state and international privacy, cybersecurity and digital technology issues. His practice covers global data protection and compliance programmes, data breaches, crisis management, consumer protection issues and internet law. Alan advises companies on cybersecurity preparedness and digital governance, and on litigation, regulatory defence, internal investigations, and policy advocacy. He handles consumer class actions, enforcement matters and public policy involving the FTC, State Attorneys General, the SEC, the FCC, the DOJ, international data protection authorities and other government agencies. Alan is a member of the American Bar Association's Cybersecurity Legal Task Force, the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the PLI's Privacy Law Advisors Group, the Council on Foreign Relations, and the governing Board of Directors of the Future of Privacy Forum.

Sidley Austin LLP

1501 K Street, N.W.
Washington, DC 20005

Tel: +1 202 736 8477
Email: araul@sidley.com
Web: www.sidley.com

SIDLEY