Fordham International Law Journal

Volume 40, *Issue* 5 2017 *Article* 9

Brexit and Implications for Privacy

Kurt Wimmer* Joseph Jones†

*

†

ESSAY

BREXIT AND IMPLICATIONS FOR PRIVACY

Kurt Wimmer[*] *& Joseph Jones*[**]

The United Kingdom is home to a vibrant technology sector, the innovations of which underpin many of the industries, products, and services that drive the European economy. Other industries in the UK, from the banking and financial sector to headquarters of global multinational companies, also depend on flows of data across national borders. The implications of the UK's withdrawal from the European Union are profoundly uncertain, and this uncertainty is particularly pronounced in the technology sector because of European regulation of data privacy and the flow of personal information.

As we show here, however, the practical impact of Brexit on key concepts of data privacy is not likely to be substantial over the long run. Like parties to a divorce, the formal ties between the UK and the

* U.S. Chair, Data Privacy and Cybersecurity Group, Covington & Burling LLP, Washington, D.C. From 2000-2003, Mr. Wimmer was managing partner of Covington's London office.

** Associate, Covington & Burling LLP, London.

EU will be unwound over the next two years. But former spouses often find that there is much to bind them even after the tie of marriage is broken, and we expect that this will be the case with the UK and the EU as well. Still, the relationship will never quite be the same.

I. BACKGROUND: EU DATA PROTECTION LAW

Under EU and UK law, data privacy is pervasively regulated. Unlike the legal structure in the United States, where sector-specific laws apply specific privacy rules to varying industry sectors, EU data protection law applies consistent principles across all types of personal information. The current law on privacy, the EU Data Protection Directive,[1] dates from 1995 and was transposed into UK law through the Data Protection Act 1998. Under the Directive, which was one of the first binding international legal instruments establishing the law of data protection, processing of "personal data" is subject to key protections meant to protect the interests of the European data subject.[2]

Key protections include a requirement that any processing be done pursuant to a "legal basis" – notably, with the consent of the subject, for the performance of a contract with the subject, to protect the subject's interests, or for the "legitimate interests" of the processor. Personal data must be processed fairly; it can only be collected for a legitimate purpose; the amount of data cannot be excessive in light of the purpose for its collection; it must be accurate; and individuals have the right to access and correct it. "Sensitive" personal data, such as data revealing racial or ethnic origin, political opinions, religious beliefs, union membership, and data concerning sexual life, is subject to greater protection. Importantly, the personal data of EU subjects can only leave the boundaries of the EU if the receiving country has legal protections that are "adequate" in the eyes of the EU.

---

1. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281/31.

2. "Personal data," under the Directive, means any information related to an identified or identifiable living person. "Processing" is defined as any operation that is performed upon personal data, whether by automatic or manual means.

The 1995 Directive was developed before the Internet was commercialized, and has struggled to remain relevant. In light of the many changes in the past 20 years, a new European regulation was crafted and will enter into force in May 2018. This new law, the General Data Protection Regulation ("GDPR"),[3] is significantly more stringent and all-encompassing than the 1995 Directive. Among other things, the GDPR enhances existing legal requirements, creates a multitude of specific new rules, extends the territorial scope of EU data protection laws, establishes a new EU-wide privacy regulator, and sets out stiff penalties for organizations that fail to comply with its provisions. Importantly, the GDPR is a "regulation" and not a "directive." Thus, it need not be transposed into national law by each Member State of the European Union, but rather will apply on its own terms once it comes into force. Assuming, then, that the UK does not formally leave the EU until mid-2019, the GDPR will be in force in the UK, as across the EU generally, prior to Brexit.

II. DIVORCE PROCEEDINGS

To achieve Brexit, the UK, on March 29, 2017, issued formal notice to leave the Union in accordance with Article 50 of the Treaty on the European Union ("TEU"). Triggering Article 50 TEU begins the two-year period (or longer if all the other EU Member States agree an extension) for the UK to negotiate the arrangements for its withdrawal (which may take into account the UK's future relationship with the EU – *see* "A new marriage"). Much like most divorce proceedings, the negotiations will focus on what happens on day one of the divorce. Even more like divorce proceedings, the Article 50 negotiations will likely focus on money, assets, shared collaborations, and who can live and stay with whom. For Brexit, this will mean addressing UK contributions to the EU budget, what to do with EU institutions physically located in the UK, shared industry sectors (e.g., nuclear), and the rights of EU citizens in the UK and *vice versa*.

Importantly, during the Article 50 negotiation period the UK remains a full member of the EU and is subject to EU law in the usual way. For privacy this means that:

---

3. Council Regulation 2016/679/EC of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. L 119/1.

The EU GDPR will be directly applicable in the UK from May 25, 2018.

The Network and Information Systems Directive ("NIS Directive")[4] will require implementing into UK law via domestic legislation by May 9, 2018.

Proposals for an e-Privacy Regulation,[5] if finalized and applicable while the UK is still a member of the EU, will form part of UK law.

The jurisprudence of the Court of Justice of the EU ("CJEU"), past and future, has primacy over UK law.

III. D(IVORCE)- DAY

The terms of the UK and EU marriage are enshrined in UK domestic legislation in the form of the European Communities Act 1972 ("ECA"). The ECA defines the legal relationship between the UK and EU principally by asserting the supremacy of EU law. More specifically, the ECA creates the following norms:

EU Treaties and Regulations apply in the UK without any further domestic implementation of those provisions by the UK into UK law.[6] For example, the four freedoms of movement (goods, people, services, and capital) over EU borders, the rights to privacy and the protection of personal data (Article 7 and 8, respectively, of the EU Charter of Fundamental Rights), and the GDPR form part of the UK *acquis* of law without anything further required by the UK.

EU Directives apply in the UK only by virtue of UK domestic legislation transposing them into UK law. The ECA obliges the UK to transpose these provisions and sets out the parameters and areas for discretion as to *how* the UK transposes and implements EU law enacted this way.[7] For example, the EU Data Protection Directive was transposed into UK law via the Data Protection Act 1998.

---

4. Directive 2016/1148/EC of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. L 194/1.

5. Proposal for a Regulation concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC, COM(2017) 10 Final.

6. European Communities Act 1972, c. 68, § 2 (UK).

7. *Id.*

International agreements concluded by the EU on behalf of its Member States apply to the UK as the UK is a Member State of the EU that has conferred the competence to conclude such arrangements with the EU. For example, the EU-U.S. Privacy Shield, the EU-U.S. "Umbrella" Agreement,[8] and the EU-Canada Passenger Name Records Agreement[9] all apply to the UK in its capacity as an EU Member State.

In order to achieve "Brexit" the UK Government will need to unpack the cornerstone that governs and authorizes the UK's membership and position in the EU. Simply, the UK will need to repeal the ECA. The UK Government has indicated that it will announce its intention to repeal the ECA via an Act of Parliament, referred to as the "Great Repeal Bill".[10] Repeal of the ECA means that all directly applicable provisions of EU law (e.g., EU Treaty provisions and Regulations) would automatically cease to apply in the UK. It also means that legislation based on the ECA (i.e., UK law that implements EU Directives) will cease to apply. If this course is undisturbed and let to run then on day one of Brexit, there will be a "cliff edge" which the UK regulatory framework will fall off. The EU *acquis* of law will disappear from the UK *acquis*. When one considers the volume of legislation and trade deals concluded by the EU in the history of the more than four decades of UK membership, this is not an insignificant *corpus* to bury. The ending of a long marriage can leave a gap that may take years to ever fill.

Cognizant of this, the UK Government proposes to "save" and "convert" the EU *acquis* of law into UK law on day one of Brexit.[11] The Great Repeal Bill, as first published by the UK Government, proposes to both repeal the ECA and at the same time transpose into

---

8. 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 Offences, 2016 O.J. L 336/3, at 3-13.

9. Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data. *See* Proposal for a Council Decision on the Conclusion of the Agreement Between Canada and the European Union on the Transfer and Processing of Passenger Name Record Data, COM (2013) 528 Final.

10. The formal title of the "Great Repeal Bill" is the European Union (Withdrawal) Bill, which was published on July 13, 2017.

11. *See* DEPARTMENT FOR EXITING THE EUROPEAN UNION, LEGISLATING FOR THE UNITED KINGDOM'S WITHDRAWAL FROM THE EUROPEAN UNION (UK). *See also* DEPARTMENT FOR EXITING THE EUROPEAN UNION, THE UNITED KINGDOM'S EXIT FROM AND NEW PARTNERSHIP WITH THE EUROPEAN UNION, § 1.1 (UK).

UK domestic law, wholesale, all EU law that applied in the UK prior to Brexit day. The rules will be the same but the legal bases for their application will derive, formally and legally speaking, not from the EU but, instead, from UK law. The proposed Great Repeal Bill has been set out but many legal and political hurdles and questions remain. But it can be said with some degree of confidence that the UK privacy framework as it exists on Brexit T-minus one day will look substantially similar to the UK privacy framework on Brexit day. The UK Government's intention is for UK to have an "unprecedented … common regulatory framework" with the EU on Day One of Brexit.

The foregoing may be true for EU *law* but what is not clear is what will happen to the UK's position vis-à-vis agreements concluded by the EU on behalf of its Member States. On Brexit, the UK will cease to be a Member State and will, therefore, fall out of scope of these arrangements. The flow of personal data will be one such complication notwithstanding UK Government intentions to ensure that the flows are uninterrupted.

IV. A NEW MARRIAGE?

A. UK-EU Data Flows

Under EU law (including the Data Protection Directive and, as of May 2018, the GDPR), data is free to flow throughout the EU so long as the data protection rules are complied with. The transfer of personal data out of the EU is restricted. Under current and future EU rules, data can be transferred to third countries only where (i) the European Commission has deemed that the recipient country's data protection regime is "adequate" (which has been interpreted to mean must be "essentially equivalent" to the regime that exists under EU law[12]) or (ii) other safeguards (like "standard contractual clauses" or "binding corporate rules") are deployed to effectively create adequacy.

Post-Brexit, the UK will be one of these third countries and an adequacy determination (or something analogous) may form part of the negotiations. Implementation of the GDPR into UK law will go

12. Schrems v. Data Protection Commissioner, Case C-362/14, 2015, ¶¶ 73—74, http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2015.398.01.0005.01.ENG.

some way to the UK showing "adequacy" but it is unlikely to be the silver bullet. The EU will take a holistic approach to determining whether the UK's privacy framework is adequate – the GDPR is but one yardstick the UK can be measured against. As was seen with the invalidation of the EU-U.S. Safe Harbor and the subsequent negotiations and challenges related to its successor, the EU-U.S. Privacy Shield, attaining adequate status may not be straightforward. The UK may face specific difficulties with respect to its domestic data retention and surveillance law and practices (which the CJEU has declared incompatible with EU law) and as to the specific manner in which it implements the GDPR (for example, the UK, as a non-member of the EU on Brexit, will have latitude to diverge from the rules and standards posited by the GDPR).

The UK being deemed adequate by the European Commission (or securing an agreement of similar effect) will ensure that organizations can move personal data from the EU to the UK. Assuming the UK implements the GDPR into UK law in substantially the same content restrictions on data transfers into its domestic law, however, the UK will also need to deem the EU's data protection regime "adequate" in order to allow data to move from the UK to the EU.

B. UK-to-Third Country Data Flows

Although the EU is the UK's largest trading partner for data, the transfer of data between the UK and other countries outside the EU is also vital for the growth and competitiveness of the UK economy.

The UK, as a member of the EU, benefits from the adequacy decisions the EU has in place for third countries such as Canada, Israel, Switzerland and the United States. The UK also benefits from arrangements that the EU has concluded with third countries that facilitate the sharing of law enforcement data (e.g., the EU-U.S. "Umbrella" Agreement) and other data sharing arrangements (e.g., the EU-Canada Passenger Name Record Agreement). On Brexit, the UK will no longer benefit from these arrangements. To ensure personal data in the UK can continue to be sent across the globe, the UK government will need to assess whether it can accede to these existing arrangements or conclude separate bilateral agreements. Maintaining and/or replicating these arrangements will be critical for data flows as well as for resolving the international legal conflicts that sometimes arise when companies honour requests for law

enforcement data. Note also that some countries have their own adequacy regimes; governments from those countries normally look to the EU's recognition of adequacy as a guide for their own adequacy decisions.

Another consideration for the UK is that the arrangements it puts in place with third countries may impact the deal the UK can conclude with the EU regarding data flows – in other words, a UK-U.S. data flow deal that flew in the face of EU rules and standards could be a blocker to a UK-EU deal.

C. Future Regulatory Regime

It would be tempting to conclude that as a divorcé, the UK can play by its own rules with respect to privacy. That is true, strictly speaking at least. Post-Brexit, the UK can take its privacy laws in whichever direction it pleases, subject to its own domestic law limitations, which the UK Parliament is sovereign to amend at any time and which will be within the jurisdiction of the UK, rather than the EU courts. That said, the reality of the UK exercising this apparent unfettered freedom will be limited and shaped by the commitments it seeks and puts in place with the EU and other third countries. The other side of the negotiating table for data flows, a priority of the UK Government, will seek to secure something close to similarity (if not "essential equivalence") in regulatory protections in UK law to that which exist in their own jurisdiction. Divergence too far one way or the other could jeopardize the UK's ability to secure the free flow of data from the UK to other countries. If data is effectively localized in the UK or if data is effectively prevented from being transferred to the UK, this will not only undermine the UK Government's aspirations for the UK to be at the forefront of the digital revolution but it will also undermine the cross-border functioning of UK companies and companies looking to do business in the UK.

D. EU Jurisprudence

Worthy of separate attention is the status of CJEU case law in the UK post-Brexit.

In its White Paper on the Great Repeal Bill, the UK Government indicated that the Great Repeal Bill will bring an end to the jurisdiction of the CJEU in the UK in a formal sense. In that sense,

UK courts will no longer be able to refer cases to the CJEU and nor will the CJEU be the ultimate arbiter on questions of UK law derived from the EU. As regards historic case law, and cognizant of the lacuna in jurisprudence of simply forgetting historical CJEU decisions, the UK Government proposes to enshrine historic CJEU case law with the "same binding, or precedent, status" in UK courts *as if* they were UK Supreme Court decisions. Tying historic CJEU jurisprudence to domestic jurisprudence means that there will can be some continued certainty in the scope and shape of rights and obligations in UK law that originally derived from EU law (e.g. on the scope of the so-called "right to be forgotten,"[13] specific application of the right to privacy, or what makes a third country "adequate" for data protection purposes[14]).

That said, UK courts and UK Parliament may, and indeed are entitled to, deviate from historic CJEU case law over time "when it appears right to do so" and it is quite probably there will be discrepancies in how UK courts and the CJEU interpret and apply similarly-phrased provisions of law. Moreover, post-Brexit CJEU decisions and interpretations will have no formal binding role in the UK courts. The exact weight that will be given by UK courts to future CJEU decisions on similarly-scoped rights and obligations to those that exist in UK law remains a great unknown, however.

V. CONCLUSION

In matters of law and policy, the letter of the law seldom tells the entire story. Expectations and norms are built up around legal structures over years of operation, and economies create their own demands and traditions. In the case of privacy in the EU, the need to ensure consistent data flows across borders is a powerful force. This is particularly true in the United Kingdom, which is a center of commerce and the technology industry for not only Europe but the world. Brexit will, to be sure, change the United Kingdom in many ways. But the remarkable force exerted by flows of data will ensure that privacy laws in the EU and the UK remain relatively consistent for both parties even after their divorce.

---

13. Google Spain v. Agencia Española de Protección de Datos, Case C-131/12, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN.

14. *Schrems*, C-362/14.