White Paper

Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation

Omer Tene, Senior Fellow
Christopher Wolf, Founder and Co-Chair
The Future of Privacy Forum

January 2013

The Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. The forum is led by Internet privacy experts Jules Polonetsky and Christopher Wolf and includes an advisory board comprised of leaders from industry, academia, law and advocacy groups.

Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation

The proposed EU General Data Protection Regulation ("GDPR")[1] re-defines EU privacy jurisdiction and applicable law. Article 3(1) of the GDPR, which deals with the authority to regulate a controller or processor located within the European Union and addresses locally-based actors, is uncontroversial in its assertion of authority. The introduction of a new "one-stop-shop" concept, with a primary regulator, to augment this "country of origin"-based approach should help provide legal certainty for organizations operating in Europe.

Article 3(2) of the GDPR extends the application of European law to the processing of personal data by a controller *not* established in the EU, where "the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behavior." This extension of extraterritorial application constitutes a dramatic shift from a country of origin to a *country of destination* approach, and portends general application of the GDPR to the entire Internet. It threatens to create uncertainty over when EU law will be deemed to apply and cause conflicts with other privacy regimes at a time when interoperability is key. Furthermore, organizations that are subject to the scope of the GDPR through Article 3(2) would not benefit from the "one-stop-shop" concept, which is a cornerstone of the new regime. This anomalous outcome, which discriminates against organizations established outside the EU, undermines the intent of the drafters to enhance harmonization and global interoperability.

Extraterritoriality under the DPD

The GDPR marks a significant expansion of the extraterritorial application of EU data protection law. As such, the new test is at odds with established EU law on when jurisdiction and application of law are appropriate. As early as in its first major decision under the Data Protection Directive ("DPD"), the European Court of Justice ("ECJ") warned that the European data protection law must not be applied indiscriminately to the entire Internet.[2] Discussing the DPD rules on international data transfers, the ECJ held:

> "[i]f Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet

[1] References to the proposed GDPR are to the European Commission proposal of 25 January 2012: Proposal for a Regulation 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 (General Data Protection Regulation), COM(2012) 11 final. References to the Rapporteur's Report are to the Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht.

[2] Case C-101/01 Bodil Lindqvist [2003] ECR I-12971.

> page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet."[3]

With respect to organizations not established in Europe, the GDPR principally changes the focus from the "use of equipment" test under Article 4(1)(c) of the DPD to govern entities outside the EU if those entities offer goods and services to *or* "monitor the behavior" of EU data subjects. This would apply regardless if such foreign entities do not have a foothold, legal or physical, in the EU. The Rapporteur's Report proposes that European law would apply even to services offered free of charge, and more broadly to "all collection and processing of personal data about Union residents" regardless of a lack of a geographical nexus to the controller or its equipment. Such an expansive approach to jurisdiction and applicable law would bring about precisely the "general application" that the ECJ tried to prevent.

This criticism is not to say that the current "use of equipment" test is the only alternative. The "use of equipment" test is a variation on the physical presence test for jurisdiction that commonly is used as a basis for regulation. Critics maintain that the location of a server is not an apt basis for regulatory jurisdiction, since a server may be remote from the place where data collection and use are having an impact. At times, despite an organization's "use of equipment" in Europe, the EU's interest in regulating such an organization's activity may be tenuous. Consider, for example, an Indonesian controller using servers in the EU to process data concerning Indonesian customers. Under the current framework, such an Indonesian controller falls under the remit of the DPD and is restricted from re-transferring data back from EU-based servers to its home jurisdiction. In addition, the broad interpretation by regulators of the "use of equipment" clause has led to its application in cases seemingly remote from the legislative intent, such as where a foreign organization with no other equipment in the EU placed a cookie on an EU user's web browser, which was deemed to be an EU-based "use of equipment".[4]

More recently, the Article 29 Working Party, analyzing the applicable law provisions under the DPD, stated that Article 4(1)(c) of the DPD could have "undesirable consequences, such as a possible universal application of EU law."[5] While this problem already existed with the "use of equipment" test in Article 4(1)(c) of the DPD, it is far more likely to arise under the amorphous "offering of goods or services" or "monitoring" tests in Article 3(2) of the GDPR.

Under Article 3(2), companies with little or no geographical nexus to the EU are effectively expected to modify their entire business models and establish elaborate internal governance schemes (including data protection officers, data protection impact assessments, restrictions on international data transfers, and more) to comply with EU law. The expectation that a

---

[3] *Ibid*, at para. 69.
[4] Article 29 Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, WP 56, 30 May 2002, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf.
[5] Article 29 Working Party, Opinion 8/2010 on applicable law, WP 179, 16 December 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

business in India or China (*e.g.*, a Chinese website that has no physical foothold in the EU, which is accessed by Chinese-speaking EU residents) will comply with a prescriptive regulatory framework established by another country is unrealistic.

Consider the opposite scenario: how would Europeans feel about India or China purporting to apply its laws (for example, on telecommunications, privacy or network security) to European companies "offering of goods or services" or "monitoring" users in its jurisdiction without being present there? Imagine the BBC coming under the remit of Chinese law and becoming subject to stiff criminal penalties based on its accessibility by English-speaking Chinese residents in China.

Lack of enforceability

The new test threatens to create conflict with other privacy regimes at a time when interoperability is key. The upshot will be inevitable difficulties in enforcing the law; an infringement on principles of comity and public international law; and unnecessary obstacles to the development of the Digital Agenda for Europe.

Geographic overexpansion will inevitably lead to unenforceability, given that the jurisdiction of EU data protection authorities does not extend beyond EU borders. Unenforceable legislation brings the law into disrepute. In the context of Article 4(1)(c) of the DPD, the Article 29 Working Party expressed its concerns about unenforceable overexpansion. It advocated a cautious approach, limiting application of European law to "those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved."[6] Similarly, Lee Bygrave warned against regulatory overreaching, "a situation in which rules are expressed so generally and non-discriminatingly that they apply *prima facie* to a large range of activities without having much of a realistic chance of being enforced."[7]

A case in point is the *LICRA v. Yahoo*, in which a French court ordered Yahoo to implement technical or access control measures to block from French users auctions featuring Nazi memorabilia, which were hosted on the Yahoo.com site.[8] Yahoo noted that in addition to Yahoo.com, which is intended for a US audience, it also operates country-specific websites including Yahoo.fr, which was customized for French users and free of Nazi-related content. At the same time, it contested the validity of the French court's order in a California court. The US court eventually ruled that the French court's decision was unenforceable given its infringement on constitutional free speech rights.[9] Similarly, in *Dow Jones & Co. v. Gutnick*, the High Court of Australia subjected Dow Jones' *Barron's* magazine to suit in Australia for

[6] Article 29 Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, WP 56, 30 May 2002, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf.
[7] Lee Bygrave, Determining applicable law pursuant to European Data Protection Legislation, 16 COMP. L. & SEC. REP. 252 (2000).
[8] UEJF et LICRA v. Yahoo! Inc. et Yahoo France, Tribunal De Grande Instance De Paris, N° RG:00/05308, May 22, 2000.
[9] Yahoo! Inc. v. LICRA and UEJF, 433 F.3d 1199 (9th Cir. 2006) (the decision later was overturned on grounds of ripeness since the French had not sought to enforce the judgment in the US; but the case illustrates the potential for conflict).

defamation in that country under Australian law arising from a web posting on a U.S.-based server.[10] This created a conflict of law as the US-based magazine became subject to multiple legal tests around the world for the same content.

In a recent article, Peter Swire has warned that with the proliferation of encryption in various communication technologies, law enforcement and national security will shift lawful access requests from local infrastructure (*e.g.*, telcos and ISPs) to records stored in the cloud.[11] Consequently, law enforcement authorities will increasingly target foreign cloud service providers, reaching out beyond their jurisdiction in an attempt to access stored individual records. If police or prosecutors do so without submitting requests through formal government channels, legal and political tensions will rise. In a recent report, the Council of Europe warned that "[t]hird parties expect to be able to operate under the rules of the State in which they are located or do business (…) transborder access could put third parties in jeopardy, both legally and practically."[12] These cases and others illustrate that even where laws could be read to apply internationally, effective enforcement often stops at the national border.

International law conflicts

International law prohibits official action by one state in the territory of another.[13] For example, a state may not carry out an investigation in another state without consent of the state where the enforcement is to be conducted, if the purpose is to enforce the first state's own administrative, criminal, or fiscal law.[14] The principle of comity has been used to limit the extraterritorial scope of domestic law in international relations; any exceptions must be based on orderly process and reciprocity. According to the OECD, the concept of "positive comity" describes a voluntary policy calling for a country to give full and sympathetic consideration to other countries' important interests while it is making decisions concerning the enforcement of its own law. "Negative comity", on the other hand, involves a country's consideration of how it may prevent its law enforcement actions from harming another country's important interests.[15] In this way, state sovereignty is respected and a

[10] Dow Jones & Co. v. Gutnick, (2002) 210 C.L.R. 575 (Austl.)
[11] Peter Swire, From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, 2(4) INT'L DATA PRIV. L. 200 (2012).
[12] Council of Europe, Cybercrime Convention Committee, Transborder access and jurisdiction: What are the options?, Report of the Transborder Group adopted by the T-CY on 6 December 2012, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf.
[13] Christopher Kuner, Submission to the "Consultation on the Commission's comprehensive approach on personal data protection in the European Union", Faculty of Law, University of Copenhagen, Denmark, 14 January 2011, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/citizens/kuner_christopher_en.pdf.
[14] Christopher Kuner, Data Protection Law and International Jurisdiction on the Internet (Part 1), 18 INT. J. L. INFO TECH 176 (2010).
[15] OECD, Committee on Competition Law and Policy Report on Positive Comity (1999), http://www.oecd.org/daf/competition/prosecutionandlawenforcement/2752161.pdf; *also see* Hilton v. Guyot, 159 U.S. 113, 164 (1895). The principle, which dates back to Roman law, was developed in the seventeenth century with the emergence in Europe of nation-states. The birth of nation-states begat the view that a sovereign's laws are limited to its territorial boundaries.

jurisdictional conflict avoided, encouraging civility in international relations.[16]

Clearly, extraterritorial application and enforcement actions should not be pursued unilaterally. Christopher Kuner writes in this respect: "Attempting to force data importers and subcontractors outside the EU to consent to the performance abroad of governmental enforcement functions (such as audits) by data protection authorities ignores the fact that the consent required is not of the entity processing the data, but of the State under whose jurisdiction it falls."[17]

A legal framework of universal application may well infringe on the sovereignty of other states, be practically unenforceable, and assign organizations with the unenviable task of choosing between overlapping, conflicting regulatory frameworks. Moreover, unilateral application of extraterritorial jurisdiction undermines the emerging concept of interoperability, which recognizes that although global privacy frameworks will continue to diverge due to cultural and historical reasons, transborder data flows can be maintained and individual rights protected.[18] This is particularly evident in the Rapporteur's Report, which in cases of a foreign government's access to data exported from the EU sets forth "an obligation, regardless of national legislation, to provide full details of all access to the data by public authorities in the third country".[19] Such notification, known in some contexts as "tipping off",[20] may compromise law enforcement efforts and constitute an outright violation of national criminal law.[21]

Purposeful targeting

The extraterritorial application of the GDPR should be revisited, so that instead of merely "offering goods or services" to or "monitoring" European individuals an organization would need to "purposefully target" EU individuals for the GDPR to apply.[22] A rich body of private international law, including international conventions and jurisprudence of the ECJ and the US Supreme Court, supports a "purposeful targeting" test.

---

[16] While less prevalent in civil law, the principle of comity has gained credence in Continental jurisprudence. *See, e.g.*, Case Kart 16/82, Philip Morris Inc. v. Bundeskartellamt [1984] E.C.C. 393 (Kammergericht) (F.R.G.), modifying Federal Cartel Office's prohibition on merger between U.S. and British tobacco companies to limit its application to the merging companies' German subsidiaries; noting that "[t]he international law requirement of mutual consideration, which in the Anglo-American legal world plays a special part as 'comity of nations' and in the European sector is also described as 'courtoisie', has particular importance in a conflict situation among the legal systems of different States, but it has not achieved the status of a customary rule of international law".

[17] Kuner, *supra* note 14.

[18] The White House, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, February 2012, pp. 31-33, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; Paula Bruening, Interoperability: analysing the current trends and developments, 100 DATA PROTECTION LAW & POLICY 12 (May 2012).

[19] Proposed amendments to Articles 15(1)(J) and 43a and recital 89.

[20] *See, e.g.*, Valsamis Mitsilegas & Bill Gilmore, The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards, 56 INT'L & COMP. L. Q. 119 (2007).

[21] *Also see* Article 43a proposed by the Rapporteur's Report, which may require a non-EU company to clear through a data protection authority, in potential breach of national legislation, any "judgment of a court or tribunal or a decision of an administrative authority of a third country [requesting] a controller or processor to disclose personal data".

[22] The Rapporteur's Report is helpful in this respect, proposing to replace the words "relating to" in Article 2 with the words "aimed at".

Article 15(1) of the Brussels I Regulation provides for jurisdiction in a consumer's domicile in cases involving consumer contracts when a party "by any means, *directs* such activities to that Member State or to several countries including that Member State…"[23] Criteria for targeting have been introduced by the ECJ in the joint *Pammer* and *Hotel Alpenhof* cases.[24] Applying the targeting test under the Brussels I Regulation, the ECJ specified the following factors *inter alia* for determining extraterritorial jurisdiction: the international nature of the activity; use of a language or a currency other than those generally used by the organization; mention of telephone numbers with an international code; use of a top-level domain name other than that of the state in which the organization is established.

In its opinion on applicable law, the Article 29 Working Party expressly supported a purposeful targeting test, stating that this "would involve the introduction of a criterion for the application of EU data protection law, that the activity involving the processing of personal data is *targeted* at individuals in the EU. This would need to consist of *substantial targeting* based on or taking into account the effective link between the individual and a specific EU country. The following examples illustrate what targeting could consist of: the fact that a data controller collects personal data in the context of services explicitly accessible[25] or directed to EU residents, via the display of information in EU languages, the delivery of services or products in EU countries, the accessibility of the service depending on the use of an EU credit card, the sending of advertising in the language of the user or for products and services available in the EU."

United States courts grappling with the question of cyberspace jurisdiction, departed from the 1945 doctrine of *International Shoe*,[26] which sought to establish "minimum contacts" with the forum so as not to "offend traditional notions of fair play and substantial justice". This later developed into a purposeful targeting test in Supreme Court cases such as *Calder*[27], *Burger King*,[28] and more recently *McIntyre*[29] and applied to the online setting in a long line of jurisprudence.[30] In *McIntyre*, the Supreme Court held that for local law to apply the proper analysis required a demonstration that a foreign organization "purposefully avail[ed] itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws."[31]

---

[23] COUNCIL REGULATION (EC) No 44/2001of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[24] Joined Cases C-585/08 and C-144/09 Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v. Oliver Heller (References for a preliminary ruling from the Oberster Gerichtshof), Judgment of the Court (Grand Chamber) of 7 December 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0585:EN:HTML.

[25] We quote the Article 29 Working Party verbatim but caution against the use of the word "accessible", lest we fall back into the trap recognized by the *Lindqvist* court of applying jurisdiction to the entire Internet. In fact, "explicitly accessible" is an oxymoron; in the context of the Web accessibility is a passive, open-ended concept.

[26] International Shoe Co. v. Washington, 326 U.S. 310 (1945).

[27] Calder v. Jones, 465 U.S. 783 (1984).

[28] Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985).

[29] J. McIntyre Mach., Ltd. v. Nicastro, 131 S. Ct. 2780 (2011).

[30] *See, e.g.*, Doe I v. Ciolli, 611 F. Supp. 2d 216 (D. Conn. 2009); For the first stages of these developments see Michael Geist, Is There a There There? Toward Greater Certainty for Internet Jurisdiction, 16 BERKELEY TECH. L.J. 1345 (2001).

[31] McIntyre, *ibid*; citing Hanson v. Denckla, 357 U.S. 235, 253 (1958).

In the tax context, under the leading model treaty of the OECD, the jurisdiction to tax business income vests in the country that hosts the "permanent establishment" of the business.[32] Article 5 of the OECD Model Tax Convention defines a "permanent establishment" as a "[f]ixed place of business through which the business of an enterprise is wholly or partly carried on." According to the official commentary to Article 5, computer equipment, such as a server, might constitute "permanent establishment" under certain circumstances; however computer data, such as a website, does not have "a location" and therefore cannot be a fixed place of business as required by the definition of "permanent establishment." Hence, under internationally accepted tax norms, organizations are not seen as operating in and subject to the tax regime of a jurisdiction unless they have a permanent establishment or at least place servers there. Here too, the "offering of goods or services" or "monitoring" tests far exceed the norms of international taxation.

No One-Stop-Shop

The new test for applicable law conflicts with the laudable goals of the principle of "one-stop-shop" or "lead authority", which is one of the most important innovations of the GDPR.[33] Unfortunately, the framework proposed in the Rapporteur's Report would water down the concept of a "lead authority", which in the Commission proposal was expressed in terms of "competence", to merely a single point of contact.[34] Moreover, unlike the rest of the GDPR, the one-stop-shop concept is not exported beyond the borders of the EU, meaning that companies that are subject to the GDPR by force of Article 3(2) yet are not established in the EU will have to continue dealing with as many as 27 national (and additional state level) regulators.[35] Indeed, Article 4(14) of the GDPR explicitly provides that a European representative, which should (under Recital 63) or must (under Article 25) be appointed by a company subject to EU law under Article 3(2) of the GDPR "may be addressed by any supervisory authority."[36] This is anomalous when viewed in the context of the legislative intent, which was to deliver "a more comprehensive and coherent policy" and to "prevent[…] fragmentation in the way personal data protection is implemented across the Union [and] legal uncertainty."[37] The one-stop-shop concept is not solely in the interest of non-EU controllers seeking predictability, but also a cornerstone of the new regime and European common market harmonization. And while failure to extend one-stop-shop to non-EU controllers may be interpreted as an intentional omission, incentivizing foreign companies to create an establishment in the EU, such a mechanism is unlikely to yield the intended results. Many non-EU controllers falling under the ambit of Article 3(2) are small and medium size enterprises, including app developers operating on a shoestring out of a

[32] OECD Model Tax Convention on Income and on Capital – An Overview of Available Products, OECD, http://www.oecd.org/tax/taxtreaties/oecdmodeltaxconventiononincomeandoncapital-anoverviewofavailableproducts.htm.
[33] Articles 4(13) and 51(2) oft he GDPR.
[34] Rapporteur's Report recitals 97-98 and Article 51(1a).
[35] Article 51(2) of the GDPR only applies "Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State…"
[36] Under the Rapporteur's Report, such a non-EU controller could be appointed a "lead authority" by the European Data Protection Board. Yet such a "lead authority" would serve merely as a single point of contact, as opposed to a uniquely competent authority. Rapporteur's Report, Article 54a(3).
[37] Explanatory Memorandum to GDPR, at p. 2.

garage.[38] These businesses are unlikely to establish in the EU even with ample regulatory incentive.

A more balanced approach would apply the one-stop-shop solution to companies not established in the EU based on the place of appointment of a designated representative under Article 25 of the GDPR. To prevent forum shopping, the GDPR could set forth criteria for selecting the designated representative's venue, such as the Member State purposefully targeted by the controller that generates the greatest amount of revenue or where the controller locates its servers, if any.

In order to streamline the operation of the one-stop-shop concept, additional clarity is needed with respect to the criteria for determining the lead authority overseeing EU-established organizations. Under the existing text, the decisive factor in determining the lead authority is the definition of the term "main establishment". Alas, the language defining "main establishment" in Article 4(14) of the GDPR is extremely vague and sets forth a multi-layered, complex test, leaving much room for inconsistent interpretation. The determination of a lead authority should be based on a set of objective criteria, consisting primarily of the location of the company's EU headquarters; but also including the location of the company within the group with delegated data protection responsibilities; the location of the company which is best placed in terms of management functions and administrative burdens to deal with data protection compliance; or the place where most decisions in terms of the purposes and the means of the processing are taken. Indeed, these criteria were set forth by the Article 29 Working Party itself for purposes of determining the lead authority for approving binding corporate rules.[39] Such criteria, if not integrated into Article 51 of the GDPR, should at least be set forth in a Recital in order to reduce legal and business uncertainties.

The Internal Dimension

One problem associated with the applicable law provision is that even with the newly established consistency mechanism, internal-EU conflicts of law may remain unsettled. While the GDPR is intended to suppress such conflicts, there remains a role for Member State legislation in areas tangential to and impacting data protection law, such as freedom of expression (Article 80), healthcare (Article 81) and labor legislation (Article 82). The variance between national legislation, coupled with an absence of intra-European rules for resolving applicable law and supervisory competence, is likely to create additional discrepancies, which the GDPR was intended to solve. In addition, even with a consistency mechanism, the approaches of national data protection authorities, each with its own enforcement and investigatory powers, are likely to vary, meaning that companies will remain subject to conflicting interpretations or applications of the law. To reduce such variance, the concept of a "lead authority" needs to be clarified ensuring that any authority that receives a complaint

[38] According to the Rapporteur's Report, the entire thrust of EU law, including the obligation to appoint a data protection officer, would apply to non-EU small and medium size enterprises (proposed amendments to Recitals 63 and 75).

[39] Article 29 Data Protection Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, WP 108, 14 April 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf.

or plans to launch an investigation is required to refer such matters to the lead authority and thereafter act as point of liaison. Finally, the GDPR's overreliance on the delegated acts and implementing provisions granted to the European Commission increases the possibility of inconsistent regulation that could adversely impact businesses seeking predictability.

Conclusion

The country of origin rule set forth by Article 3(1) of the GDPR is sound; overextension of EU law to apply to the entire Internet is excessive. Such a move will result in a framework, which is unenforceable and infringes upon principles of comity, interoperability and international law. The "offering goods or services" and "monitoring" tests should be replaced with a purposeful targeting test, which is better aligned with existing jurisprudence in the EU and US as well as jurisdictional clauses in other consumer protection and tax legislation. In addition, the "one-stop-shop" concept needs to be extended to apply to non-EU controllers falling under the scope of the GDPR by means of Article 3(2). In order to operationalize the one-stop-shop concept, clear criteria are needed to help determine the location of the main establishment of a controller. Finally, the concept of a "lead authority" needs to be clarified to ensure that any authority that receives a complaint or plans to launch an investigation will refer such matters to the lead authority. In this respect, the Rapporteur's Report is a step in the wrong direction, shifting from the designation of a lead authority as a focal point of competence to its reduction to a single point of contact.