



Hogan  
Lovells

# GMCO

Global Media Technology and  
Communications Quarterly

Spring 2019

## Editorial

---

In our first issue of 2019 we include a round-up of our thought leadership from across the firm on issues facing clients this year, including the impact of the GDPR, the new EU Copyright Directive, a milestone in the Commission's digital market strategy and the challenges spurring M&A activity in the TMT sector.

When President Trump signed into law, in March 2018, the U.S. Cloud Act, which clarifies U.S. law enforcement's ability to reach data stored abroad, it sparked considerable discussion in the international community and was widely criticized. We include an extract of a paper written by partners Winston Maxwell and Mark Brennan and Senior Associate, Arpan Sura, which seeks to demystify the Cloud Act, evaluate the merit of various criticisms made against it and point out why the claims are overstated and in some cases inaccurate.

2019 sees the global impact of the EU General Data Protection Regulation (GDPR) in force. We include an extract from a journal article written by our Paris partners Winston Maxwell and Christine Gateau, proposing a criteria for setting administrative fines under the GDPR. This is set alongside a comment from our Dutch partner Joke Bodewits on the Dutch Data Protection Authority's approach.

We then have two articles from our Washington Communications Practice. The first is an article by Washington partner Trey Hanbury, and Senior Associate Sarah Leggin, on the lessons to be learnt from the U.S. FCC proposed fine against Viaero Wireless for violating spectrum rules. The second is a report from the Silicon Valley Smallsat Symposium, which featured leading innovators and experts from around the world and where panels were moderated by Hogan Lovells' partner Randy Segal and Counsel Tony Lin.

This month the Council of the European Union adopted the EU Copyright Directive, part of an overall package of measures which is aimed at modernising EU copyright laws for the digital age and falls within the EU Commission's ongoing digital single market strategy. On p26 we include an in-depth analysis, by our DSM taskforce, of the two most controversial provisions of the new laws: the new press publishers' right and the new liability regime for content sharing services.

We have two partner interviews. London M&A partner and co-head of the firm's global TMT industry group, Peter Watts, talks about the challenges spurring M&A activity in the TMT sector and gives his predictions for 2019. Hong Kong partner Mark Parsons talks about IoT, the development of cybersecurity and privacy regulations in Asia post the implementation of the GDPR in Europe and the changes anticipated for 2019.



**Winston Maxwell**  
Partner  
Paris



**Trey Hanbury**  
Partner  
Washington, D.C.



**Penelope Thornton**  
Senior Associate  
London

## Contents

Demystifying the U.S. CLOUD Act	4
A point system for setting administrative fines under the GDPR	12
Dutch Data Protection Authority sets GDPR fines structure	18
Two days, U.S. FCC fine of \$20,000 for violating spectrum rules	20
A big year for smallsats	22
EU copyright reform: navigating the new press publishers' right and liability regime for content sharing services	26
Big deals, big ideas, and big challenges spur activity in the TMT sector – Q&A with Peter Watts	32
Privacy, cybersecurity, and the internet of things in Asia – Q&A with Mark Parsons	35
China issues its fourth draft patent law, after over three years of deliberation	38
References	40



# Demystifying the U.S. CLOUD Act

Winston Maxwell and Mark Brennan and Arpan Sura have prepared a paper discussing the impact of a new U.S. law – the Clarifying Lawful Overseas Use of Data Act (“CLOUD Act”) – on non-U.S. businesses and individuals who use cloud storage solutions. The CLOUD Act amends the Stored Communications Act (“SCA”), which restricts the disclosure of stored electronic data to third parties, including the U.S. government. The paper specifically focuses on Part 1 of the CLOUD Act, which clarifies that U.S. law enforcement agencies may, under certain circumstances, lawfully demand data stored in foreign countries from entities subject to U.S. jurisdiction.<sup>1</sup> Some commentators have worried that Part 1 of the CLOUD Act will give the U.S. government new powers to surveil the data of any non-U.S. citizen or business that uses a cloud services provider with operations in the United States. The paper concludes, however, that such worries are overstated in at least two respects. Part 1 of the CLOUD Act does not represent a radical change; rather, it largely clarifies that a settled body of pre-existing case law applies to the SCA. Nor do the authors expect the CLOUD Act to enhance the capacity of U.S. law enforcement to collect non-US citizens’ data stored outside the U.S.; there are numerous legal and practical safeguards in place that would prevent such an outcome. In this issue we include an extract from the paper. To read the full paper visit: <https://bit.ly/2Dyx90s>

On March 23, 2018, President Trump signed into law the Clarifying Overseas Use of Data Act (“CLOUD Act”).<sup>2</sup> The CLOUD Act amends a U.S. privacy law known as the Stored Communications Act (“SCA”), which restricts the disclosure of stored electronic data to third parties, including the U.S. government. The CLOUD Act contains two important provisions. First, it requires that certain Internet-based service providers subject to U.S. jurisdiction “disclose the contents of an electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside

of the United States” (“Part 1 of the CLOUD Act”).<sup>3</sup> Second, the CLOUD Act allows foreign governments to enter into new bilateral Executive Agreements (“EAs”) with the United States. These EAs would permit streamlined foreign law enforcement requests directly to U.S. service providers and would complement the procedures in existing Mutual Legal Assistance Treaties (“MLATs”) and common-law principles of international comity (“Part 2 of the CLOUD Act”). No EAs are yet in effect. This paper examines the first part of the CLOUD Act, the part that states that the location of data is not relevant for purposes of production orders issued under the SCA.



By clarifying U.S. law enforcement's ability to reach data stored abroad, the CLOUD Act sparked considerable discussion in the international community.<sup>4</sup> Some commentators in the European Union, for example, criticized the CLOUD Act as a threat to global civil liberties. They warned that the CLOUD Act would expand U.S. government access to the data of EU citizens and businesses. Businesses in the EU, meanwhile, worried that the CLOUD Act would threaten the privacy and security of their data hosted or stored on cross-border cloud networks.

A few common themes have emerged from these disparate criticisms: the CLOUD Act is a novel expansion of U.S. power; it will jeopardize territorial sovereignty; and it will undermine the privacy interests created by jurisdiction-specific laws, such as the General Data Protection Regulation ("GDPR") in Europe.

This paper evaluates the merit of these claims and finds them overstated and in some cases inaccurate. Assessing the impact of the CLOUD Act on global cloud solutions requires a proper understanding of: (i) the background statute – the SCA – that the CLOUD Act amended; and (ii) the Second Circuit's decision in *Microsoft v. United States* that caused the U.S. Congress to pass the CLOUD Act in response. Read against this backdrop, the CLOUD Act largely reaffirmed the established legal view – namely, the court in the *Microsoft* decision misinterpreted the SCA by adopting a bright-line rule based on the data's physical location. The prevailing legal authority interpreting the SCA examines whether the recipient of a request has "possession, custody,

or control" of the data, not whether the data is physically located outside the United States. The "possession, custody, or control" criteria are flexible, allowing judges to evaluate the specific facts surrounding each criminal investigation. These flexible criteria are part of international standards in the field of criminal investigations, appearing in Article 18 of the Council of Europe's Cybercrime Convention.

A proper understanding of the SCA also shows why the CLOUD Act does not undermine key privacy protections. The SCA allows U.S. law enforcement to obtain data under limited circumstances – for example, the SCA applies only to certain types of service providers subject to U.S. jurisdiction, and it requires probable cause before a judge can issue a warrant for certain stored content. The CLOUD Act has not changed these legal requirements for lawful access, which are also consistent with EU fundamental rights standards.

The rules of criminal procedure generally seek to avoid bright-line legal tests that would make it easy for suspected criminals to move evidence to convenient hiding places outside the country. That is one of the reasons why the physical location of data servers has become largely irrelevant under rules of criminal procedure, as courts and law enforcement authorities apply a more flexible and fact-specific standard like article 18 of the Council of Europe's Cybercrime Convention. That flexibility is then counter-balanced by robust procedural and human rights protections to avoid judicial and prosecutorial overreaching.

“

A proper understanding of the SCA also shows why the CLOUD Act does not undermine key privacy protections.

”

### Back to the Future: The CLOUD Act restores the functioning the SCA as it existed for decades

The expressed concerns of some EU stakeholders appear to be grounded on the notion – however vague – that the CLOUD Act gives the U.S. government expansive new power over data stored all over the world. But that fear is inaccurate and misplaced. The CLOUD Act is not a departure from prior precedent. Its core provision overturns the Second Circuit’s *Microsoft* decision and instead sides with the majority of prior court decisions that reject *Microsoft*’s reasoning. These courts had held that the physical location of the data does not matter under the SCA so much as the party who controlled it. “Control, not location” has been the prevailing rule, notwithstanding *Microsoft*, and the CLOUD Act simply confirms the rule.<sup>5</sup> Before examining *Microsoft* in detail, some background about the SCA is necessary. The Stored Communications Act permits the government to compel an “electronic communications service” (“ECS”) or “remote computing service” (“RCS”) – including a cloud service – to disclose its customers’ data to law enforcement under certain circumstances.<sup>6</sup> Although the statute’s requirements are discussed in greater detail below, three broad limitations on the Act’s scope are worth noting at the outset.

First, courts have held that the SCA limits law enforcement to data that an ECS or RCS has in its “possession, custody, or control.”<sup>7</sup> That is the same standard that applies to civil discovery – including international e-discovery – in the United States.<sup>8</sup> Under the “possession, custody, or control” test, the “location of the information sought is irrelevant.”<sup>9</sup> That is also the relevant test under the Council of Europe’s Cybercrime Convention, as we discuss in Section IV.

Second, the SCA includes a number of additional statutory safeguards that meet or exceed the protections afforded under the U.S. Constitution. For example, it does not apply to an entity that is not an ECS or RCS. Moreover, the SCA provides that law enforcement may obtain the contents of communications





stored<sup>10</sup> for less than 180 days only if it satisfies the traditional requirements for a search warrant, governed by the Fourth Amendment to the U.S. Constitution and Federal Rule of Civil Procedure 41.

Third, notwithstanding the SCA's protections, some courts have held that law enforcement requests for the contents of communications are *always* "searches" within the meaning of the Fourth Amendment, no matter how long the communications have been stored. That means that the government must show "probable cause" to believe that the information sought will contain evidence of a crime.

### ECS/RCS requirement

The SCA imposes another statutory restriction on U.S. law enforcement – the recipient of a lawful recipient warrant, subpoena, or other request must be an RCS or ECS. If the recipient is not an RCS or ECS, then the request is invalid under the SCA. Whether an entity qualifies as an RCS or ECS is context-specific, and an entity can be an RCS or ECS (or both) with respect to some data but not others.

The term "remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communication system."<sup>11</sup> To be an RCS, a company essentially must offer value-added data storage services to the public. The statute's legislative history explains that such services exist to provide sophisticated and convenient data processing services to subscribers and customers, such as hospitals and banks, from remote facilities.<sup>12</sup>


There are two key limitations on whether an entity qualifies as an RCS.

First, a company does not become an RCS solely because it stores data incidental to its primary business. For example, a defendant that stored a client's employees' personal information was held not to be an RCS with respect to that data; storage was incidental to the defendant's main service of providing the employees with a way to purchase household goods through payroll deductions.<sup>13</sup> Similarly, an airline that compiled and stored passenger information and itineraries through its website was not an RCS, because these functions were incidental to providing airline reservation service.<sup>14</sup> Likewise, an e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users."<sup>15</sup>

Second a company does not provide an RCS to the extent it is not available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example, an employer that provides email accounts to its employees is not an RCS with respect to those employees' data, because such email accounts are not available to the public.<sup>16</sup> As another example, Pandora's cloud music streaming service was not deemed an RCS because there was no allegation that users could upload or store content.<sup>17</sup>

An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or





photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.”<sup>18</sup> An ECS generally provides user access to a central computer system through which to send electronic messages over telephone or other communications lines. While the typical ECS includes internet service providers, email providers, and bulletin boards, it is possible for an online business or retailer to become an ECS if it has a website that offers customers the ability to send messages or communications to third parties.<sup>19</sup> In other cases that do not involve messaging services, courts regularly conclude that ordinary businesses providing services through the Internet are not an ECS.<sup>20</sup>

### **Jurisdictional requirements**

Under the SCA and the Due Process Clause of the U.S. Constitution, a warrant or subpoena may be directed to an ECS or RCS only if that entity is subject to “personal jurisdiction” in the United States.<sup>21</sup> The concept of “personal jurisdiction”<sup>22</sup> (which arises under the U.S. Constitution) is distinct from the concept of “territorial jurisdiction” (which is implicated, for example, under the CLOUD Act). At a high level, the question of “personal jurisdiction” asks whether a person or company has sufficient “contacts” with a forum to be subject to its authority. The questions of to what extent a non-U.S. citizen or business is subject to U.S. jurisdiction in any particular case are highly dependent upon the particular facts of each matter.

Independent of the CLOUD Act, then, a warrant or subpoena under the SCA cannot reach a company over which the court lacks “personal jurisdiction.” Therefore, a U.S. court may lack “personal jurisdiction” over a U.S. or foreign entity, even if that entity exercises “control” over the data stored overseas under the CLOUD Act.

### **“Possession, custody, or control” requirement**

The CLOUD Act clarifies that an RCS or ECS served with legal process under the SCA must turn over data that is within



its “possession, custody, or control,” regardless of where such data is stored:

“A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.”<sup>23</sup>

The “possession, custody, or control” standard has been extensively litigated in other contexts, namely the Federal Rules of Civil Procedure. Rule 34 provides that records may be sought where they are in the “possession, custody, or control” of a party to the litigation.<sup>24</sup> While the terms “possession” and “custody” are fairly straightforward (basically amounting to physical possession), the legal definition of “control” is far less clear. In the context of document requests served on corporations, U.S. courts have generally applied one of two competing tests to determine if records possessed by a non-party corporate affiliate or independent third party can be considered to be within the party’s “control.”<sup>25</sup>

Most courts today apply a broad equitable standard known as the “practical ability” test. This is a multi-factored analysis under which a court will generally order document production if it “find(s) that a company’s ability to demand and have access to documents in the normal course of business gives rise to the presumption that such documents are in the litigating corporation’s control.”<sup>26</sup> Numerous courts have applied a multifactor test and held that a U.S. subsidiary can have control over documents stored by its foreign parent.<sup>27</sup> Some of these factors include: (1) commonality of ownership; (2) exchange or intermingling of directors; (3) the exchange

of documents in the ordinary course of business; (4) the non-party’s connection to the transaction at issue; (5) any benefit or involvement by the non-party corporation in the matter; (6) a subsidiary’s marketing and/ or servicing of the parent company’s products; and (7) the financial relationship between the companies. A minority of courts conduct a narrower inquiry relating to control known as the “legal right” test, which defines “control” under Rule 34 as “the legal right to obtain documents requested upon demand.”<sup>28</sup> Under this stricter approach, the party’s practical ability to obtain the documents is irrelevant absent legal entitlement.

The control test is necessarily flexible and fact-specific, which is understandable in the context of criminal investigations, where criminal defendants may attempt to keep incriminating evidence outside the reach of U.S. prosecutors.

Regardless of the standard used, the “possession, custody, or control” test continues to be a substantive limitation on document discovery requests. As one example, one court found that a parent corporation did not exercise the level of control over its subsidiary necessary to have “control” over its documents for Rule 34 purposes.<sup>29</sup> In that case, the court concluded that “while (the parent’s) ownership of its subsidiaries is a factor favoring plaintiffs in their bid for the foreign subsidiaries’ documents, the lack of any track record in which (the parent] has actually exerted control points in the opposite direction.”<sup>30</sup> It did not, as the court pointed out, participate in its subsidiaries’ decision-making or monitor their activities, and furthermore did little “to independently verify the financial information they provide as inputs to (the parent’s) consolidated financial statements.”<sup>31</sup>

As these cases make clear, the “possession, custody, or control” test constitutes a meaningful constraint

“

The CLOUD Act does not change the fundamental structure – let alone reduce the substantive data protections – of the Wiretap Act or other privacy laws unrelated to the SCA.

”

on law enforcement requests for data held by a non-U.S. entity under the CLOUD Act.

#### a. No direct access to data

The SCA establishes a legal process that regulates the ability of U.S. law enforcement to order RCS and ECS providers to disclose evidence. The SCA requires U.S. government entities to meet certain standards of proof to obtain the customer information of an RCS or ECS. These standards will depend on the type of information sought. The SCA does not allow law enforcement to extract data directly from systems, and the CLOUD Act does not eliminate or modify these procedural safeguards.

To access contents of electronic communications – including emails – that have been in electronic storage for less than 180 days, the SCA requires the government to obtain a search warrant from a judge.<sup>32</sup> One court has recently articulated that standard as follows: “Probable cause to search a location exists if, based on the totality of the circumstances, there is a “fair probability” that evidence of a crime may be found there.”<sup>33</sup>

Thus, where there is no “fair probability” of evidence relating to a crime, the SCA does not permit U.S. law enforcement to obtain the email. The probable cause standard is one of the highest under U.S. law with regard to law enforcement. It derives from the Fourth Amendment of the U.S. Constitution and

governs, among other things, wiretaps and police searches of homes or cars.

The government may obtain non-content records (e.g., network logs) or emails that have been stored for longer than 180 days through a subpoena or a “court order” issued under the SCA,<sup>34</sup> both of which require a lower showing than probable cause. The requirements for subpoenas vary by jurisdiction and statute, but they generally require that the subpoena be designed to produce documents relevant to a lawful investigation. Similarly, an SCA court order can be issued only if the records sought “are relevant and material to an ongoing criminal investigation.”<sup>35</sup> Here again, U.S. law enforcement must show some nexus to a crime.

Independent of the SCA and the CLOUD Act, some courts have held that the Fourth Amendment to the U.S. Constitution requires a warrant based on “probable cause” for law enforcement to obtain stored email. The leading authority, *Warshak*, held that a warrant is necessary to obtain emails under the SCA’s procedures, and “to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.”<sup>36</sup> In the wake of *Warshak*, it has been the policy of the U.S. Department of Justice since 2013 to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process.<sup>37</sup>

Moreover, the U.S. Prosecutors' handbook prepared by the Department of Justice regulates how federal prosecutors should handle cross-border data requests. The handbook makes clear that prosecutors must advance with great care and get clearance from the Criminal Division's Office of International Affairs.<sup>38</sup>

As we discuss in Section IV, moreover, the "probable cause" threshold for SCA warrants protects individuals to a similar extent as EU laws on fundamental rights. In the context of their review and criticisms of the former Safe Harbor regime, the European Commission and European Court of Justice have never raised concerns regarding the U.S. regime for criminal investigations.

Neither the SCA nor the CLOUD Act displace other methods of seeking information from service providers; rather they add extra restrictions before an ECS or RCS can disclose customer information. If a law enforcement request or an administrative agency request is for information stored on a server subject to the SCA, the request will be subject to the SCA.

But beyond the SCA, Congress has imposed stricter requirements on specific types of searches. For example, the Wiretap Act allows U.S. law enforcement to engage in wiretapping and electronic eavesdropping, but only in connection with the investigation of certain enumerated crimes.<sup>39</sup> Furthermore, the Wiretap Act requires that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved.<sup>40</sup>

The CLOUD Act does not change the fundamental structure – let alone reduce the substantive data protections – of the Wiretap Act or other privacy laws unrelated to the SCA.

## b. The five layers of SCA filters must all be satisfied

In summary, the SCA as modified by the CLOUD Act, incorporates five cumulative layers of filters, all of which must be satisfied:

- The entity targeted must be an RCS or ECS;
- The entity targeted must be under the personal jurisdiction of U.S. courts;
- The evidence sought must be under the "possession, custody, or control" of the targeted entity;
- Law enforcement must follow legal process, including establishing "probable cause" for certain content; and
- The application of the warrant must not violate the CLOUD Act's statutory comity framework or principles of international comity as expressed in the *Société Nationale Industrielle Aérospatiale* case.



**Winston Maxwell**

Partner, Paris Office  
+ 33 1 53 67 48 47  
winston.maxwell@hoganlovells.com



**Mark W. Brennan**

Partner, Washington Office  
+ 1 202 637 6409  
mark.brennan@hoganlovells.com



**Arpan A. Sura**

Senior Associate, Washington Office  
+ 1 202 637 4655  
arpan.sura@hoganlovells.com

# A point system for setting administrative fines under the GDPR

In an article written for La Revue Des Juristes De Sciences Po, Hogan Lovells partners Winston Maxwell and Christine Gateau consider the criteria for setting administrative fines under Article 83 of the GDPR, in light of the European Data Protection Board (“EDPB”) Guidelines, the case law of the CJEU and national courts. Where applicable, Maxwell and Gateau compare the criteria in Article 83(2) of the GDPR with those used in setting administrative fines for competition law violations, as well as with the methodology used by authorities in the United States for setting fines. Maxwell and Gateau also consider procedural safeguards under Article 6 of the European Convention on Human Rights. In this issue we include an extract from the article. To read the full article visit: <https://bit.ly/2UX1TmD>

Article 83 of the GDPR<sup>41</sup> provides for two levels of administrative fines: a lower level – maximum €10 million or 2% global turnover – for violations relating to record-keeping, data security, data protection impact assessments, data protection by design and default, and data processing agreements; and a higher level – maximum €20 million or 4% global turnover – for violations relating to data protection principles, the legal basis for processing, information to data subjects, the prohibition of processing sensitive data, denial of data subjects' rights, and data transfers to non-EU countries.

In addition to setting two levels of administrative fines, Article 83 of the GDPR provides criteria that national supervisory authorities must apply when setting administrative fines. On October 3, 2017, the Article 29 Working Party – a body now called the European Data Protection Board – issued guidelines (“EDPB Guidelines”) on the setting of administrative fines.<sup>42</sup>

“

Evoking the level of damage suffered by data subjects is always difficult because many data protection violations correspond to harms that are not easy to measure in economic terms.

”





Pursuant to the EDPB Guidelines, supervisory authorities must consider the proportionality of corrective measures mentioned in Article 58(2) of the GDPR, including a warning or reprimand, before imposing a fine. When supervisory authorities conclude that an administrative fine is necessary, we propose that they refer to a scoring system that would provide a common framework for calculating the amount of the fine. The scoring system would be based on the number of persons affected by the violation, and would include various multipliers designed to reflect the nature, gravity and duration of the infringement. The score would then be adjusted by the mitigating or aggravating factors listed in Article 83(2) of the GDPR.

Supervisory authorities would remain free to adjust, or in some cases disregard, the scoring system to take account of the facts of each case. But a common framework for calculating fines would contribute to transparency, consistency and legal certainty.

### The principle of equivalence

The first principle mentioned in the EDPB Guidelines is that sanctions should be “equivalent”. The principle of equivalence flows from Article 57(1)(g) of the GDPR, which requires that supervisory authorities cooperate “with a view to ensuring the consistency of application and enforcement of this Regulation”. Recitals 10 and 11 of the GDPR also stress the need for equivalent sanctions. According to the EDPB, equivalence requires that different supervisory authorities in the EU apply similar fines to similar cases. The principle of equivalence can also be found in the case law of the European Court of Justice, but the meaning is not exactly the same as that mentioned by the EDPB. In CJEU case law on sanctions, the concept of equivalence means that Member States must apply sanctions to violations of EU law that are equivalent to sanctions applicable to comparable violations of national law.<sup>43</sup>

The GDPR’s mechanisms on cooperation and consistency<sup>44</sup> ensure that supervisory authorities

coordinate their actions, particularly for violations involving cross-border processing. Article 70(k) of the GDPR empowers the EDPB to create guidelines on corrective measures and administrative fines in order to ensure consistency. In its Guidelines, the EDPB points to its dispute-resolution powers under Article 65 of the GDPR as a way for the EDPB to help ensure consistency in fining practices. However, the EDPB’s dispute-resolution role would come into play only when one supervisory authority objects to another’s proposed sanction, and that would only occur for sanctions that fall under the coordination and consistency mechanism for cross-border processing.

Finally, equivalence requires that a supervisory authority apply the same level of sanctions to the same kind of violation, i.e. non-discrimination in the application of sanctions. The non-discrimination obligation is part of the constitutional obligation of predictability and legality of sanctions.

### “Effective, proportionate and dissuasive” sanctions

Article 83 states that administrative fines under the GDPR should be “effective, proportionate and dissuasive”. These criteria appear explicitly in a number of other EU directives and regulations.<sup>45</sup> The concepts “effective, proportionate and dissuasive” flow from Article 4(3) of the TEU, which requires that Member States take all measures necessary to guarantee the application and effectiveness of Union law. Thus even if the words “effective, proportionate and dissuasive” were not expressly mentioned in Article 83 of the GDPR, the concepts would nevertheless apply to administrative fines under the GDPR.<sup>46</sup>

Effectiveness, proportionality and dissuasiveness have been defined by CJEU case law. “Effectiveness” means that national law should not render the enforcement of EU law virtually impossible.<sup>47</sup> Effectiveness also includes the

principle of equivalence and non-discrimination as regards comparable violations of national law.<sup>48</sup> “Proportionality” means that sanctions should not exceed what is appropriate and necessary to attain the objective legitimately sought by the legislation, and that when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.<sup>49</sup> The obligation to consider all appropriate measures and choose the least onerous is also reflected in the EDPB’s Guidance: Supervisory authorities “**must** include consideration of all the corrective measures, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own”.<sup>50</sup> “Dissuasiveness” means that the application of the penalty must result in the party having violated the law being substantially worse off than would be the case if he complied with the law. This requires, at a minimum, that the penalty be sufficiently high so that the guilty party loses any benefit that arose because of the illegal behaviour.<sup>51</sup> Dissuasiveness also requires that one take into effect the likelihood of enforcement:

“89. A penalty is dissuasive where it prevents an individual from infringing the objectives pursued and rules laid down by Community law. What is decisive in this regard is not only the nature and level of the penalty but also the likelihood of its being imposed. Anyone who commits an infringement must fear that the penalty will in fact be imposed on him. There is an overlap here between the criterion of dissuasiveness and that of effectiveness.”<sup>52</sup>

The European Competition Authorities Working Group on Sanctions confirms this approach to deterrence:

“In order to achieve an adequate level of deterrence, the level of fines should exceed any potential gains that may be expected from the infringement”.<sup>53</sup> When discussing the concept of “effective, proportionate and dissuasive” fines, the EDPB Guidelines do not cite any of the CJEU case law referred to above. The EDPB states simply that “[a] more precise determination of effectiveness, proportionality or dissuasiveness will be generated by emerging practice within supervisory authorities (on data protection, as well as lessons learned from other regulatory sectors) as well as case-law when interpreting these principles”.<sup>54</sup>

## The “nature, gravity and duration” of the infringement

Article 83(2)(a) of the GDPR requires that administrative fines take account of the “nature, gravity and duration” of the infringement. As pointed out by the EDPB Guidelines, the GDPR already creates two categories of infringement: those attracting a lower maximum fine (€10 million/ 2% global turnover), and those attracting the higher maximum fine (€20 million/ 4% global turnover). These two levels of maximum fines correspond to violations of different provisions of the GDPR. The lower maximum fines correspond to violations of security obligations and record-keeping obligations, among others. The higher maximum fines correspond to violations of articles going to the heart of the GDPR's substantive obligations, such as the obligation to have a legal basis for processing, or to inform data subjects about processing. By setting different maximum fines, the GDPR signals that violations of the second series of articles are more serious than violating the first series of articles. Thus Article 83 already provides an initial classification of violations according to their nature and gravity: the violations mentioned in Article 83(5) GDPR, which correspond to the highest potential fines (4% global turnover), have a “nature and gravity” score potentially twice as high as the violations mentioned in Article 83(4), which correspond to the lower maximum fines (2% global turnover).

A logical conclusion would be that fines for violations mentioned in Article 83(5) should generally be twice as high as fines for violations mentioned in Article 83(4). However, this rule of thumb would in many cases conflict with other rules of Article 83, including the rule of proportionality or the rule that fines should take account of the level of damage suffered by data subjects. For example, violations relating to data security obligations are listed in Article 83(4) and therefore benefit from a relatively low score for “nature and gravity”. Yet data security violations can create extremely high damages for data subjects; they are among the gravest form of GDPR violation in terms of adverse consequences for data subjects and society. By contrast, a failure to include the

duration of data retention in an information notice will in itself cause little or no damage to data subjects and can be considered a form of technical violation. Yet failure to mention the duration of data retention corresponds to a violation of Article 13 that falls under Article 83(5), and therefore attracts a higher “nature and gravity” score than a massive data security breach.

Consequently, the classification between different kinds of violations in Article 83(4) and 83(5) does not provide a reliable benchmark for assessing “nature and gravity”. A more reliable proxy for gravity would be the number of data subjects affected, multiplied by the level of damage suffered by each data subject. A violation involving sensitive data, or resulting in identity theft, might correspond to a higher damage score for each individual than a violation creating no damage, for example a failure to mention the duration of data retention in an information notice. The level of gravity could therefore be measured by multiplying the number of affected data subjects by an individual damage score. For example, in the case of a data breach involving the loss of sensitive data for 100,000 data subjects, the number of data subjects may be multiplied by a high individual damage score, for example 3. This would yield a nature and gravity score of  $100,000 * 3 = 300,000$ .

Evoking the level of damage suffered by data subjects is always difficult because many data protection violations correspond to harms that are not easy to measure in economic terms. Recital 75 GDPR lists the many forms of the harms that can result from data protection violations, and while it is difficult to put a price tag on many of the harms mentioned in Recital 75, it is possible to create categories of harm, for example, light, medium and severe. This sort of classification is required in any event for data protection impact assessments, where the adequacy of protective measures will depend on the risk of harm. The risk of harm must necessarily take into account the level of impact on each data subject.

Article 83(2)(a) states that in addition to taking into account the number of data subjects affected and the level of damage suffered by them, supervisory



Given the human rights focus of the GDPR, data protection authorities are not accustomed to attributing economic values to data protection violations.



authorities should also consider “*the nature, scope or purpose of the processing concerned*”. A purpose for data processing with a high level of utility for society, e.g. medical research, might warrant a lower multiplier than a purpose with lower societal benefits, e.g. commercial advertising. In the context of our example, let us imagine that the processing of sensitive data was done for the purpose of creating commercial profiles for advertising. This would generate a high purpose multiplier, for example 3, compared to processing for medical research, which would generate a low purpose multiplier of 1. Thus in the foregoing example, the nature and gravity score would again be multiplied by 3:  $300,000 * 3 = 900,000$ .

In addition to the nature and gravity, the duration of the violation must also be taken into account. Adding duration to the formula is straightforward: It would be sufficient to add a multiplier to the equation corresponding to the number of months during which the violation occurred. In the above example, if the data vulnerability resulting in the loss of sensitive data lasted for 6 months, the resulting nature and gravity score (900,000) would be multiplied by 6, the number of months during which the violation occurred. A linear duration multiplier is routinely used in setting of competition law fines.

The EDPB Guidelines do not suggest using a simple duration multiplier. Instead, the EDPB says that the duration will be an indication of:

- “a) wilful conduct on the data controller’s part, or
- b) failure to take appropriate preventive measures, or
- c) inability to put in place the required technical and organisational measures.”<sup>55</sup>

As our example above shows, creating a consistent methodology for scoring nature, gravity and duration is relatively straightforward. More difficult will be transforming the score into a monetary penalty. Should each point in the score correspond to an administrative fine of 0.20€, 0.50€, 1€, or 2€? We will return to this question in section 6 below.

### “Minor” infringements

Recital 148 of the GDPR refers to the concept of “minor infringements”, which the EDPB explains may be infringements that in the particular circumstances do not pose a significant risk to the rights of data subjects, and do not affect the essence of the obligation in question. For minor infringements, Recital 148 states that a “reprimand may be sufficient”. This corresponds to the requirement, mentioned in section 2 above, that supervisory authorities systematically consider application of all alternative remedies in Article 58, and choose the one that is most proportionate in the





circumstances. A failure to mention the duration for the retention of data in the information notice may be an example of a minor infringement, particularly if the actual retention periods for data used by the data controller are not excessive. By contrast, a failure to mention the duration of data retention combined with excessively long data retention periods would likely be viewed as affecting the “essence of the obligation in question”. The violation would in that case not be a minor infringement for purposes of Recital 148.

## Conclusion

The principles of “effective, proportionate and dissuasive” sanctions have been interpreted by the CJEU, and those interpretations will naturally apply to sanctions imposed under the GDPR. The principle of proportionality, in particular, requires that supervisory authorities consider the full range of corrective measures and choose the one that is least intrusive while still permitting the attainment of the objectives of the GDPR. In many cases, a warning or reprimand will be sufficient.

When a fine is considered necessary, we suggest that the EDPB develop a methodology for calculating the amount of the fine, based on a point system. This approach has been used for competition law sanctions, and increases transparency, consistency and legal certainty of sanctions. A major difficulty in the context of GDPR will be translating the point system into economic units corresponding to fines. Competition law violations can be measured in economic terms. Data protection violations are more difficult to measure economically. Therefore the competition law approach cannot be transposed as-is to the GDPR. Given the human rights focus of the GDPR, data protection authorities are not accustomed to attributing economic values to data protection violations. Yet translating violations into monetary amount is inevitable when setting administrative fines, so supervisory authorities will need to find a common method for doing so,

particularly because fines are likely to become large under the GDPR.

The scoring system we suggest in this article is based first on the number of data subjects affected by the violation. A violation affecting 3 people would have a lower score than a violation affecting 3 million. Various multipliers would then be applied to this initial score, to reflect the seriousness of the violation, the kind of data involved, the purpose of the processing, and the duration of the infringement. Once an adjusted score is obtained, supervisory authorities would then apply the aggravating and mitigating factors listed in Article 83(2) of the GDPR. In appropriate cases, supervisory authorities could decide to modify the point system, or even disregard it entirely, to reflect the particular circumstances of the case. However, without a common scoring system, setting administrative fines will be based on intuitive and subjective factors that will undermine the GDPR's objective of consistency and predictability.



**Winston Maxwell**

Partner, Paris Office  
+ 33 1 53 67 48 47  
winston.maxwell@hoganlovells.com



**Christine Gateau**

Partner, Paris Office  
+ 33 1 53 67 18 92  
christine.gateau@hoganlovells.com

# Dutch Data Protection Authority sets GDPR fines structure

On 14 March 2019, the Dutch data protection authority (Autoriteit Persoonsgegevens, DPA) announced its fining structure for violations of the European General Data Protection Regulation (GDPR) and the Dutch law implementing the GDPR (Implementation Act). Joke Bodewits analyses the detail.

The GDPR sets two levels of administrative fines that may apply depending on which GDPR provisions have been infringed: the higher of €10 million or 2% of global revenue and the higher of €20 million or 4% of global revenue. At both levels, the GDPR sets maximums for administrative fines and calls on member state authorities to determine what fine is appropriate in individual cases.

The Dutch DPA has introduced the four categories as set out in the table below. While the Dutch DPA has set default fines for violations in each category, it also has set a range to be applied depending on the specifics of a violation.

Category of fines	Range	Default fine
Category I	€0 and €200.000	€100.000
Category II	€120.000 and €500.000	€310.000
Category III	€300.000 and €750.000	€525.000
Category IV	€450.000 and €1.000.000	€725.000

“

The Dutch DPA will diverge from the default amount listed if there are either mitigating or aggravating circumstances, such as the nature, severity and duration of the violation.

”

The first category is reserved for simple violations such as not sufficiently keeping records of the responsibilities of processors or joint controllers, and not publishing the contact details of the Data Protection Officer (DPO).

The second category is reserved for not fulfilling certain requirements for processing such as not concluding data processing agreements with processors, not securing personal data well enough, not conducting impact assessments, or guaranteeing the DPO's independence.

Examples of the third category include violations of the transparency requirement, failure to notify of data breaches, and not cooperating with the Dutch DPA.

The fourth category is reserved for the unlawful processing of special categories of data (including the national identification number) unlawful profiling, and not complying with specific orders from the Dutch DPA.

Interestingly, categories I and II do not correspond to violations that are punishable by the lower GDPR fine of €10 million, nor do categories III and IV solely correspond to violations that are punishable by the GDPR fine of €20 million.

The Dutch DPA will diverge from the default amount listed if there are either mitigating or aggravating circumstances, such as the nature, severity and duration of the violation, amount of affected individuals and the scope of the damages. Most importantly, if the amount is deemed not to be fitting, the Dutch DPA can still impose the maximum fine of €20 million or 4% revenue.



**Joke Bodewits**

Partner, Amsterdam Office

T +31 20 553 3645

[joke.bodewits@hoganlovells.com](mailto:joke.bodewits@hoganlovells.com)

# Two days, \$20,000 for violating spectrum rules

In February 2019, the U.S. Federal Communications Commission (“FCC”) proposed a \$20,000 penalty against Viaero Wireless (“Viaero”) for allegedly transmitting in the 3650-3700 MHz band without an authorization. The fine highlights the importance of ensuring compliance with rules on spectrum use.

In April 2015, the FCC reformed the licensing regime governing the 3650-3700 MHz band (“3.5 GHz band” or “Citizens Radio Broadband Service”) to expand commercial use of the spectrum.<sup>56</sup> CBRS is designed to benefit many markets and applications by making private LTE wireless networks more economically and technically feasible, offering unlicensed spectrum without cost, and allowing wireless carriers to add coverage and capacity to boost data rates, among other uses.

The FCC adopted a novel “layer cake” spectrum sharing regime in the band. CBRS has a three-tiered hierarchy of users, which gives Tier-1 services (U.S. Navy radars, fixed satellite earth stations) priority over Tier-2 Priority Access License (“PAL”) services, who in turn have priority over Tier-3 General Authorized Access (“GAA”) users. Tier-2 PALs will be assigned using competitive bidding. Tier-3 GAA users have no protection and may use spectrum at the risk of interference from others in the band. The Spectrum Access System will manage the system of sharing. CBRS licensees’ compliance with all license and registration requirements is crucial to the success of CBRS given the many operators sharing the same resource and the pyramid of protections operators must respect.

The FCC’s Enforcement Bureau is the primary FCC unit responsible for enforcing the provisions of the Communications Act, the Commission’s rules, orders, and various licensing terms and conditions. Viaero is a fixed wireless Internet and mobile broadband Internet provider serving Colorado, Kansas, Nebraska, and Wyoming for more than 25 years. It offers wireless service

“

This decision underscores the importance of knowing the service rules that apply to each band and ensuring compliance with them.

”



throughout the rest of the United States through roaming partnerships with the leading nationwide providers. The decision provides a good reminder to know the service rules that apply to each band and ensure compliance with them. It also shows that even well-established providers may make mistakes.

The proposed penalty against Viaero arose through the FCC's standard enforcement process. The FCC received a complaint of interference from a licensed and registered station in the band on February 8, 2018, and dispatched a field agent to investigate the issue a few days later. The field agent reportedly confirmed Viaero was transmitting from an unregistered station, and contacted Viaero to stop. Viaero complied, according to the Bureau.

Roughly one month later, the Bureau sent a Notice of Violation to Viaero directing the company to provide more information about the unauthorized transmissions.<sup>57</sup> In response, Viaero admitted to transmitting for approximately two days without first registering its station and without coordinating with other licensees before operations. Viaero also told the FCC it had since registered its station and would not operate until completing frequency coordination with other licensees in the band. The FCC's records confirm Viaero's registration.

In February 2019, the Bureau issued a Notice of Apparent Liability for Forfeiture ("NAL"), which advised Viaero how it had violated the law and the amount of the proposed penalty.<sup>58</sup> The FCC found Viaero violated its Part 1 and Part 90 rules, which prohibit the operation of unauthorized/unregistered stations.<sup>59</sup> In the 3650-3700 MHz band, a licensee cannot operate a station before registering it and coordinating with other licensees in the band in order to prevent harmful interference to others sharing the band, including the future CBRS.

The Bureau tentatively found that Viaero violated the FCC's Part 1 and Part 90 rules,<sup>60</sup> and proposed a fine of \$20,000, the base forfeiture penalty established by its Part 1 rules (\$10,000 fine for operation without an authorization per day).<sup>61</sup>

The FCC's Part 1 rules allow it to impose penalties for rule violations, subject to limitations on the amount, the factors the FCC must consider when determining the appropriate penalty, and the discretion it may execute under the statute.<sup>62</sup> According to Viaero,

its operations team simply assumed that its station had been registered and conducted testing for about two days when it had not. Given the totality of the circumstances, the Bureau found no upward or downward adjustment was warranted. The Bureau gave Viaero the standard 30 days from the release of the notice to pay the forfeiture penalty (until March 11, 2019), or, alternatively, file a written statement supported by documentation and affidavits seeking reduction or cancellation of the proposed forfeiture.

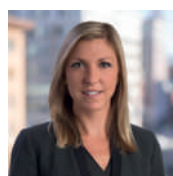
This decision underscores the importance of knowing the service rules that apply to each band and ensuring compliance with them. In this case, the FCC established CBRS in 2015 to support flexible wireless broadband use, including industrial applications and even national defense missions.<sup>63</sup> The FCC recently said the CBRS band was so important it seemed poised to become "an essential part of next generation wireless network deployments, including 5G, around the world."<sup>64</sup>

No matter the band or the FCC's policy priorities at play, prompt corrections, transparency, and engagement with the FCC following a misstep can help mitigate the risk of large penalties if an operator discovers a violation – even if the unauthorized operation may have resulted from an innocent mistake. Viaero's responsiveness to the Bureau and corrective actions may have prevented the FCC from imposing a higher fine this time. But operators should note that the Bureau said "action in this area against unregistered operators is essential" because unregistered stations "undermine the Commission's primary mission to manage radio spectrum."<sup>65</sup>



**Trey Hanbury**

Partner, Washington Office  
T +1 202-637-5534  
trey.hanbury@hoganlovells.com



**Sarah Leggin**

Senior Associate, Washington Office  
T +1 202 637 3621  
sarah.leggin@hoganlovells.com

# A big year for smallsats

The 2019 Smallsat Symposium in Silicon Valley featured leading innovators, experts, and entrepreneurs from around the world who discussed the expanding opportunities for funding, launch, and partnerships in the smallsat industry. Tony Lin and Sarah Leggin report the conference highlights optimism and diversity in the growing smallsat Industry.

“Smallsats” are satellites that are smaller than conventional satellites – weighing around 5-10 kg and usually built as 3-unit or 6-unit cubes between 10 cm x 10 cm x 30 cm and 10 cm x 20 cm x 30 cm, respectively. Smallsats require substantially less time and cost to produce compared to conventional satellites, and offer continuous global coverage, opening up new opportunities for the commercial sector to participate in the space economy.

Using constellations of small, next-generation satellites, smallsat operators are changing the way we see the world, and leveraging that data to help understand and change it for the better. For example, Planet Labs is an earth imaging operator with over 130 satellites in orbit. Planet can image anywhere on Earth daily at high resolution. Spire Global is a data and analytics company that collects data from space to solve problems on earth. It was one of the first providers to prove concept to NASA, has 72 satellites in orbit with global coverage, and over 30 earth stations around the world. Astro Digital designs, builds, and operates small satellite systems supporting “Mission as a Service” business applications including earth observation, communications and various space manufacturing applications. Currently, Astro Digital has 5 satellites in orbit.

In a keynote address, Mike Safyan, VP Launch for Planet Labs, highlighted Planet’s victories and challenges in its first 10 years and presented an inspiring vision of Planet’s future. Like its competitors, Planet faces challenges including spectrum coordination with government users and other commercial satellite operators, unpredictable launches and limited launch schedules, and the mechanical engineering, orbit planning, and data processing challenges that come with innovative space technologies.

“

If regulators and governments create an environment with enough certainty to drive both growth and innovation, the smallsat industry is poised to deliver significant benefits for years to come.

”

Yet, stakeholders across sectors echoed his optimism about the coming years for the smallsat industry. Hogan Lovells' own Randy Segal, Corporate Partner and co-leader of the firm's Space and Satellite Practice, moderated two panels focused on new developments poised to accelerate the industry's growth. The first focused on the Smallsat Sandbox. Panelists offered perspectives on how smallsats complement, compete, and interact with other platforms, reflecting the diversity of companies within the industry. The panelists agreed that the industry is in a very exciting period where many stakeholders are experimenting with different views of what the future will look like. Some predicted that high altitude platforms, drones, and other technologies may emerge more prominently to provide competing earth imaging, weather

tracking, and disaster monitoring and response services. Others hoped that the industry would take steps toward establishing interoperability so that satellites may offer more of a seamless experience among providers.

Randy's second panel focused on the cost-savings and tailored launch opportunities presented by small launch vehicles. The panelists – most of whom were looking forward to completing their first launches later this year – agreed that they will need to remain flexible and keep adjusting to the demands of the industry. Some even predicted smallsats will get larger again especially if the small launch vehicle market fails to emerge in a meaningful way.

On the last day of the conference, Hogan Lovells' Tony Lin, Counsel in the firm's Communications,



From left: Randy Segal, Hogan Lovells; Dan Hart, Virgin Orbit; Dr. Tom Markusic; Tim Ellis, Relativity; Jim Cantrell, Vector; Dr. Giulio Ranzo, Avio

Internet and Media Practice, moderated a panel on standards and regulation. Tony noted it was fitting that this was the final panel, given that regulatory compliance is often the last thing on an operator's mind. While several panelists suggested that the regulatory framework in the United States should be relaxed to foster innovation and faster deployment, the panelists also recognized the need for some regulation as the smallsat industry matures. For example, Tahara Dawkins of NOAA said that for certain satellite systems that pose a higher national security risk, such as those capable of remote sensing (earth imaging), clear rules and regulatory oversight is necessary, while a lighter touch may be appropriate for systems that pose less risk. Other panelists urged operators and other industry stakeholders to coordinate to develop technology standards (akin to LTE and 4G in the terrestrial wireless industry) to promote interoperability. Panelists also said orbital debris issues should be regulated, but debated whether those rules should come from Congress, the Federal Communications Commission, or another agency. Panelists did agree that no regulator should try to pick winners and losers as the industry is still growing and changing.

The 2019 Smallsat Symposium set the stage for what the next year holds for smallsats. The industry will spur technological advances and change not only in the NewSpace economy, but also in telecommunications, production chains, big data analytics and other cutting-edge industries. If regulators and governments create an environment with enough certainty to drive both growth and innovation, the smallsat industry is poised to deliver significant benefits for years to come.





From left: Tony Azzarelli, Azzurra Telecom Ltd; Tahara Dawkins, NOAA; Brian Weimer, Sheppard Mullin; Brad Kizzort, Peraton; Chuen Chern Loo, ITU; Tony Lin, Hogan Lovells



**Tony Lin**  
Counsel, Washington Office  
T +1 202 637 5795  
tony.lin@hoganlovells.com



**Sarah Leggin**  
Senior Associate, Washington Office  
T +1 202 637 3621  
sarah.leggin@hoganlovells.com

# EU copyright reform:

## navigating the new press publishers' right and liability regime for content sharing services

On 26 March 2019 the EU Parliament voted to pass the draft Copyright Directive (the “Directive”) into EU law. It was adopted by the EU Council (representatives of Member State governments) on 15 April 2019. After official publication, the EP’s adopted text will become EU law. Member States will then have until mid-2021 to implement it into their national laws. In this article we take a deep dive into the two most controversial provisions in the new Copyright Directive: the new press publishers’ right (Article 15, formerly Article 11) and the new liability regime for content sharing services (Article 17, formerly Article 13). For our detailed overview of the whole Directive, see our blog <https://www.hlmediacomms.com/2019/02/26/dsm-watch-eu-copyright-directive-the-big-picture/>.

### Article 17 (formerly 13): the new liability regime for content sharing services

The Commission’s stated aim of Article 17 is to “reinforce the position of creators and right holders to negotiate [a licence] and get remunerated for the use of their content by certain user-uploaded content services”.

When an online content-sharing service provider gives access to copyright-protected content uploaded by its users, Article 17 provides that it performs an act of communication to the public or an act of making available to the public and those acts must be authorised by the rightholder (e.g. by concluding a licensing agreement). This has been a controversial and heavily debated aspect of the Directive because it makes some online services primarily liable for copyright infringement in relation to the acts of their users.

While the online content sharing services are urged to conclude licensing agreements with right holders or get their authorisation, it is expressly stated that rightholders are free to refuse to grant authorisation. This aspect of Article 17 has been criticised for curtailing the freedom of the internet because if rightholders do not grant a licence for specific works infringement liability cannot be avoided unless the content sharing service can meet the 4-step criteria set out below.

“

The complexity of Article 17, the vagueness of the assessment criteria, and its sheer length however has drawn criticism from all sides.

”



Where authorisation has also been obtained it will cover the acts carried out by a service's users when they are “not acting on a commercial basis” or when their “activity does not generate significant revenues” It is not clear what “significant” revenues means in this context. Where is the threshold? Would small influencers generating only a couple of hundred Euros per month be covered, or only those who make a living from their activity?

### Who is caught?

Article 2(6) defines an “online content sharing service provider” as an online service “whose main or one of the main purposes is to store and give the public access to a large amount of copyright protected works [...] uploaded by its users which it organises and promotes for profit-making purposes.” For ease, we shall refer to such a service as a “content sharing service”.

Recital 63 states that the assessment of what amounts to a “large amount” must be made on a case-by-case basis, depending on a non-exhaustive list of criteria (e.g. audience size and amount of copyright-protected files uploaded). Explicitly excluded from the definition are not-for-profit online encyclopedias (e.g. Wikipedia); not-for-profit educational and scientific repositories; open-source software developing and sharing platforms (e.g. GitHub), ISPs, online marketplaces, B2B and personal cloud services. However, discussion forums (hosting comments) or dating platforms (hosting pictures) could arguably be covered by the definition.

Since there is no threshold, it could be argued that any profits made by the platform operator could be sufficient to make it fall within the scope of the definition regardless of the amount. A small platform operated by one person which allows its users to share their pictures and which generates through advertising barely enough revenues to be self-sufficient is treated much the same as the most popular platforms out there. To deal with this, the Directive includes a lighter regime for start-ups (see further below).

### Unlicensed Content: the four-step limitation of liability regime

Content sharing services currently benefit from the safe harbour regime under Article 14(1) of the e-Commerce Directive, which provides that service providers are not liable for the content they store if they (a) have no knowledge of the illegal nature of the content they store, and (b) act expeditiously to remove the flagged content upon notification (notice and take-down).

However, content sharing services cannot rely on the safe harbour regime in relation to the acts covered by Article 17 (i.e. giving the public access to copyright protected works uploaded by users) (Article 17(3)). Instead, the regime set out in Article 17 will apply to such acts.

A generally applicable regime for avoiding liability for content unlawfully uploaded by their users is set out in Article 17(4). Content sharing services must be able to demonstrate they are fully compliant with a 4-step process:

- Step 1: they have made best efforts to obtain an authorisation from the right holders; and
- Step 2: they have made “in accordance with high industry standards of professional diligence” best efforts to ensure the unavailability of specific works identified by rightholders; and in any event
- Step 3: they have executed notice and take down requests expeditiously; and
- Step 4: they have made best efforts “in accordance with high industry standards of professional diligence” to prevent the future upload of content which has been the subject of a notice and take down request (i.e. notice and “stay” down).

Where there is no licence in place for a work, rightholders must supply content sharing services with the necessary information to identify the work and submit sufficiently substantiated take down requests. If they don't, the content sharing service will not be liable for the availability of that work on its service (Article 17(4) and Recital 66, §3).

### Meaning of “best efforts”

A central element of the regime is the concept of best efforts, or more specifically “best efforts in accordance with high industry standards of professional diligence”. In making an assessment of the latter, for the purposes of steps 2 and 4 (ensuring unavailability of works), the recitals make clear that account should be taken of “all the steps that would be taken by a diligent operator to achieve the result of preventing the availability of unauthorised works [...] on its website”. Account should be taken of best industry practices and the effectiveness of the steps taken in light of all relevant factors and developments, as well as the overall principle of proportionality. When considering the effectiveness of any steps, a number of factors should be taken into account including the type, the audience and size of the service, the evolving state of the art of existing means and the costs for service providers. Any steps should be effective but not go beyond what is necessary to avoid the availability of works.

These criteria are supposed to allow for a finely-tuned mitigation of liability regime, properly adapted to the concrete situation of each content sharing service. However, with so many factors to (potentially) consider confusion on how to implement the steps is highly likely. Recital 71 does state however that, as soon as possible after the Directive comes into force, the Commission should organise dialogues with stakeholders to define best practices with regard to the appropriate industry standards of professional diligence. Some guidance should therefore be provided in time.

It is not clear whether any of the above criteria are also relevant to assessing what amounts to best efforts to obtain authorisation. Questions therefore remain as to what a content sharing service must do. Is a content sharing service compelled to do everything in its power to get a licence, and from whom? How is a content sharing service supposed to know what content to get a licence for, and from which right holder? Does it depend on the type, audience and size of the service? The answers are not straightforward.

### Lighter regime for start-ups

The negotiators have carved-out a lighter regime (Article 17 (6)) for content sharing services:

- whose services have been available to the EU public for less than three years,
- whose annual turnover is below €10 million, and
- whose average number of monthly unique visitors does not exceed 5 million.

Such content sharing services need only comply with step 1 of the general regime (i.e. make best efforts to obtain an authorisation from the right holders), and to respond expeditiously to notice and take down requests. Content sharing services who meet the time and turnover criteria, but whose popularity exceeds 5 million, must also comply with step 4 (i.e. notice and stay down) of the general regime. It is not clear however which standard of “best efforts” applies to the acts of these content sharing services.





## Preservation of Users Rights

One of the main criticisms of Article 17 is that it will result in legitimate content being inadvertently blocked, as a result of the use of filtering technology, which cannot judge whether content can benefit from an exception (e.g. quotation, parody, etc.).

As a result, the agreed text (Article 17(7) and (9)§3,) now specifically provides that the application of Article 17, and especially the cooperation between right holders and content sharing services, must not affect the legitimate uses of works, especially those covered by an exception or limitation of copyright, and must not result in the blocking of non-infringing content. The challenge remains, however, for content sharing services to comply with the obligations of Article 17 whilst ensuring that lawfully uploaded content is not blocked.

The text also provides (Article 17(9)§§1-2) that a content sharing service must put in place a mandatory complaint and redress mechanism, by which users can contest content sharing service decisions to remove or disable access to content they uploaded. The mechanism must be “effective and expeditious”, and the complaints “processed without undue delay” (Recital 70). In addition, human review is mandatory for final decisions to remove or disable access to uploaded content.

## Comments

One of the stated aims of Article 17 is to tackle the legal uncertainty regarding the liability of content sharing services for the acts of their users. The complexity of the different mechanisms, the vagueness of the assessment criteria, and its sheer length however has drawn criticism from all sides. Further, it is hard to see how the regime will be properly harmonised across the various Member States when there is so much scope for interpretation when Member States come to implement the Directive into national laws. Overall, it hardly seems a satisfactory outcome for either content sharing services or rightholders, that the final text includes a provision that the Commission must issue guidance on the application of the Article 17, and specifically the limitation of liability regime. This practice-oriented document will be interesting, as it should contain more precise suggestions of technical solutions to comply with the limitation of liability regime but it will not be binding on the CJEU, leaving uncertainty for both content sharing platforms and rightholders. We expect that national Courts and ultimately the CJEU will have to answer a number of questions, including, in particular, what amounts to “best efforts” in relation to the various obligations on content sharing services and also precisely which services fall within the definition of an online content sharing service.

## Article 15 (formerly 11): the new press publishers' right

The very heart of the new Article 15 is an extension to press publishers of certain rights granted by Directive 2001/29/EC (the “InfoSoc Directive”). Once the Directive is implemented into national laws, publishers of press publications will have the exclusive right of reproduction, right of communication to the public and the right of making available to the public regarding the online use of press publications. This new exclusive right (granted by Article 15(1)) will

“

After years of heated debate the new right for publishers can surely be regarded as a milestone in the endeavour to create a fair system that seeks to compensate publishers for the digital uses of their works.

”

mean the targeted news aggregators and media monitoring services will have to obtain licences prior to using the affected content.

Article 15 seeks to ensure that not only press publishers but also the authors of the journalistic works themselves are compensated fairly. This is enshrined in Article 15(5) and supplemented by Article 16 of the Directive. This says that in the event that the author has transferred or licensed his rights to the publisher, Member States may provide that such a transfer or a licence constitutes a sufficient legal basis for the publisher to be entitled to a share of the compensation for the uses of the work. The revenues are intended not only to benefit the creatives, but also the publishers.

### What is caught?

The definition of press publications covers journalistic publications, published in any media in the context of an economic activity. By contrast, the protection does not affect websites, such as blogs, that provide information as part of an activity which is not carried out under the initiative, editorial responsibility and control of service provider, such as a news publisher.

Nor do the new publishers' rights apply vis-à-vis individual users (at least if used for non-commercial purposes).

Hyperlinking is also exempted from the scope of protection. However, this exception likely means “pure” hyperlinking and probably does not apply to snippets of the relevant text (with embedded links).

Interestingly, the proposal also exempts the use of individual words and very short extracts from the scope of protection. Although the agreed text has been improved over earlier drafts in this respect, a similar system was adopted in Germany in 2013, which led to considerable confusion about the material scope of the law.

### How long do the new rights last?

The exclusive rights for publishers expire two years after publication, counting from the first of January following publication date. This limitation was inserted because of concerns expressed regarding the freedom of information.

### Welcome changes

The adopted text of the Directive takes into account many points of criticism on the Commission's proposal originally published in late 2016. In particular:

- Article 15 is now only aimed at online use and no longer affects the offline sector.
- An exception has been inserted for the use of individual words or very short extracts.
- The term of protection has been reduced from 20 to 2 years.
- Blogs will not fall under the protection of press publishers.
- It no longer catches non-profit institutions and private individuals.
- It no longer applies to works published before its entry into force.

### Comparison: Germany, France, UK

While Article 15 will no doubt be celebrated by big publishing companies as a breakthrough, for the EU as a whole, the new exclusive right is no stranger to the German Copyright Act. As noted above, in 2013, a similar ancillary copyright for press publishers was implemented. That prohibited operators of search engines and news operators from making press articles or extracts of them publicly available without prior licensing. However, in Germany the new law did not lead to the intended benefits for press publishers. As the law exempts “single words and smallest text excerpts” from the general prohibition, there is legal uncertainty with respect to the interpretation of the scope of this regulation, which has resulted in numerous court actions.

Nevertheless, the German law served as a model for Article 15 in many respects: the exception for short text excerpts, fair payment for authors and the clarification that rights of the authors remain untouched by the rights of the press publishers and may not be used against them. However, Article 15 differs significantly in one important aspect: under German law, the ancillary copyright exists only for a period of one year from publication, not two years.

In France, there is no corresponding ancillary copyright law. For this reason, France—as is well known – initially also opted against the introduction of such a right at European level.

The UK currently has no such ancillary copyright for press publishers and as things stand today there must be doubt as to whether there will be in the future as a result of the Directive. That's because the UK's obligation to implement the Directive will depend on whether the UK exits the EU before or after it comes into force.

### Comments

After years of heated debate the new right for publishers can surely be regarded as a milestone in the endeavour to create a fair system that seeks to compensate publishers for the digital uses of their works.

However, while big publishers will mainly welcome this new development it remains to be seen how beneficial smaller press publishers will find Article 15, given their (relatively) weaker commercial negotiation position.

Questions also remain as to the scope of the carve out for use of individual words or very short extracts of a press publication, and lengthy judicial proceedings on this issue can be predicted with some confidence. It also remains to be seen how search engines and other service providers will react and whether, in particular, they will withdraw their news services from the European market, as occurred in Spain when it introduced a similar law, or whether the prediction of Günther Oettinger, who presented the first proposal shortly before leaving his post as European Commissioner for Digital Economy and Society, will come true that Europe as a whole is too important in this context.



**Morten Petersenn**

Partner, Hamburg Office

T +49 40 41993291

morten.petersenn@hoganlovells.com



**Alastair Shaw**

Counsel, London Office

T +44 (0) 207 296 2573

alastair.shaw@hoganlovells.com



**Penny Thornton**

Senior Knowledge Lawyer

London Office

T +44 (0) 207 296 5665

penelope.thornton@hoganlovells.com



**Benedikt Luthge**

Associate, Hamburg Office

T +49 40 419930

benedikt.luethge@hoganlovells.com

# Big deals, big ideas, and big challenges spur activity in the TMT sector

## Q&A with Peter Watts

Hogan Lovells' Partner, Peter Watts, discusses how intense innovation, diverse deal structures, and political protectionism are changing the face of M&A in the technology, media, and telecommunications (TMT) space.

### Q: What are the main drivers for cross-border deals at the moment?

**A:** There are number of long-term drivers in the TMT sector. The first is the relentless pace of innovation across all aspects of the industry. And innovation can take a number of different forms. For example, lots of deals have been driven by acquiring particular data analytics or machine learning (AI) capabilities.

Innovation is not confined to technology itself – innovation is also changing how content is distributed. So, we are seeing the explosive growth of subscription VOD services versus traditional broadcast media.

We have long been grappling with convergence between tech, media, and telecoms. As important in recent quarters is convergence between tech and a wide range of other sectors – pharmaceutical companies acquiring cutting edge technology firms or acquiring new capabilities in mobility.

Finally we shouldn't forget that old-fashioned consolidation plays are driven by a number of factors. The underlying rationale are time-honored – a wish to expand one's footprint; to leverage existing assets; to bring in new assets that drive economies of scale; or a desire to consolidate customers.

“

With protectionism apparently on the rise, TMT deals are going to be an increasing focus for regulatory scrutiny.

”





**Q: What do you think has been the most interesting deal of the last six months, and why?**

**A:** It's hard to look further than the Sky/Comcast deal. It's particularly interesting because, first, it illustrates the rapid evolution of a sector where business models are changing very quickly. And, second, it demonstrates the globalization of content consumption in a way we haven't seen before. Not long ago, Sky was a disruptive insurgent in traditional broadcasting markets; now it is an incumbent which was fought over by two global giants – each looking for a strategy to counter the media insurgency from Silicon Valley. Similar factors are driving valuations and will almost inevitably drive more deals across the media sector.

**Q: With innovation as a major driver of deals, do you feel that M&A is the best way for companies to nurture that kind of innovative spirit?**

**A:** Many deals that we observe or are involved in are about innovation in its truest sense. The TMT sector contains a vast number of companies that can create a new product or service, but don't have the skills, capital, or network to really exploit that invention – they are inventors but not innovators. In the good deals, established players with global networks, skills, and resources, can take those inventions to the next level.

If we look back over the past five to ten years, a lot of companies including some of the West Coast tech leaders, have made acquisitions in which they have bought a company or product as part of a strategy to drive that product further forward as part of a wider portfolio.

Of course, a minority of deals end up stifling innovation but they are definitely the exception rather than the rule.

**Q: Does the drive for innovation differ across other sub-sectors?**

**A:** Parts of the sector are fundamentally driven by a constant process of creating new output – whether a TV show, video game, or online content. So it is about talent and revenue rather than capital investment which can deliver returns over the long term. These businesses are constantly innovating – after all their fundamental planning horizon is the next season rather than the next decade.

But talent can be fickle and is often driven by a sense of ownership and control as much as by pure financials. So, these acquisitions can also be more challenging than in the more technology-driven end of the business where innovation is often about constantly refreshing a portfolio of long term assets.

**Q: What are the major challenges to M&A in the sector?**

**A:** TMT can generate real political sensitivities. The idea of a foreign company acquiring a media outlet with domestic cultural significance, a technology company which handles cybersecurity defenses, or a telecoms company which is critical to national connectivity is always going to raise political questions. With protectionism apparently on the rise, TMT deals are going to be an increasing focus for regulatory scrutiny.

There are also some signs that increasing valuations may be cooling the level of enthusiasm in some

parts of the market for deals at the more speculative end of the spectrum. Over the last five years we have seen a boom in companies across the economy “gambling” on investment in a portfolio of tech start-ups in the hope of securing a foothold in the next wave of technology driven innovation. This has driven tech values to a level where even buying chips in the casino has become very expensive.

Both these trends would tend to suggest some shift in the direction of travel being back towards strategic partnerships. Deals which can address regulatory and cultural sensitivities by balancing the global and the local can enable established players to combine with creative talent to drive innovation.

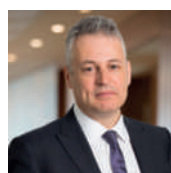
A further complicating factor is the pace of innovation. The attitude of regulators is changing fast because they are having to try to keep up with continuous change in the marketplace. For example, in October 2018, the UK Chancellor of the Exchequer, Philip Hammond, spoke about how the UK policy on large technology platforms is going to evolve. This is a debate about the role of large platforms, fake news, and new forms of economic dominance which is going on all around the world.

Regulators, even absent a protectionist thrust, are having to face a new set of challenges. For the TMT sector, there is a risk of a perfect storm of regulators, who are already faced with some very tricky questions, having to deal with cross-border acquisitions that raise questions about national sovereignty.

**Q: What advice do you have for companies looking to do deals in the sector?**

**A:** As pricing rises and regulatory hurdles increasingly influence outcomes, TMT companies who are looking to do deals will need to continue to exercise discipline on the assets they are seeking, as well as in how they engage with advisors to address regulatory hurdles early in the process. Not just with the sort of traditional antitrust functions, but also with their public policy and their broad regulatory thinking.

The challenges from issues such as monopolies, fake news, and data abuse, coupled with intense scrutiny from regulators mean that the public policy function and the transactional team, which traditionally have been a bit separate and culturally a bit different, have to start thinking together.



**Peter Watts**

Partner, London Office

T +44 20 7296 2769

[peter.watts@hoganlovells.com](mailto:peter.watts@hoganlovells.com)

# Privacy, cybersecurity, and the Internet of Things in Asia

## Q&A with Mark Parsons

Increasing numbers of initiatives, devices, and solutions related to the Internet of Things (IoT) are substantially impacting the development of cybersecurity and data privacy regulations throughout Asia. After the implementation of the GDPR in Europe, for example, Asian lawmakers are considering strengthening their own data protection laws. The region is also characterized by a push in a number of jurisdictions towards data localization requirements driven more by “cyber sovereignty,” national security considerations, and protectionist impulses than data protection considerations. Restrictions on the collection and free use of data may pose a challenge for IoT models, particularly if data is required to be kept onshore. At the same time, it is clear that many Asian jurisdictions see IoT as a key driver for economic growth. A number of jurisdictions have “smart city” initiatives and interests in areas such as automotive telematics. Japan, South Korea, and China, in particular, have strong automotive sectors and are focused on maintaining technological leadership. Unmanned aerial vehicles (UAV) are also an area of focus, both in terms of the supply of vehicles and components and in terms of their deployment as part of these “smart” initiatives. Mark Parsons, a Hogan Lovells partner based in Hong Kong, summarizes the current status of IoT-related policies in the Asia-Pacific region and discusses changes anticipated in 2019.

### **Q: Will Europe’s stringent data protection regulations have an impact in Asia?**


**A:** Definitely. We have observed a trend toward comprehensive, European-style data protection regulation here in the Asia-Pacific region for over a decade now and the introduction of the GDPR has given lawmakers fresh cause to consider if they have gone far enough in this direction.

China introduced an information security specification in May of 2018, which borrows quite heavily from the GDPR in terms

of substance. It’s a nonbinding national standard, but we’re finding that enforcement authorities are referring to it when enforcing more generally worded provisions found in mandatory Chinese laws. And India – also a significant economy in the region – has tabled a draft privacy act that also borrows heavily from a number of the innovations in the GDPR.

This is important to IoT considerations, and the rise of mandatory data breach notification laws in the region is a significant development. As an example, we now have six jurisdictions with mandatory regimes. We have volunteer





regimes in three of them, and quite likely a number of these volunteer regimes will harden into mandatory regimes in the coming years.

A key consideration for these breach notification laws is the threshold for notification – do data subjects have to suffer harm in order for the breach to be notifiable, or is any leakage of personal data notifiable? Part of the European influence we are seeing is in the movement from a harm-based threshold to the standard under the GDPR. We see that influence in South Korea, the Philippines, and a number of other jurisdictions that have put in place mandatory regimes. So again, there are very significant developments on that front.

**Q: Have data localization requirements in Asia impacted data protection and cybersecurity laws?**

**A:** We are very focused on the emergence of data localization requirements. There are businesses with IoT offerings that just will not work unless they locate servers in jurisdiction (and obtain necessary licenses to do so). This can be a significant cost and a very important operational constraint for IoT models in the region.

We see China as the most significant marker on this front, where for a year and a half now we've had a localization measure under the cybersecurity law that has not yet been fully specified. We are still awaiting the fine print on who this measure applies to and what the procedures are in terms of complying with it. We're seeing similar movements toward localization in other markets, such as Indonesia. The new draft Indian law also contains a form of localization measure.

**Q: How does China's regulatory landscape compare to others in the region?**

**A:** China's data regulation landscape is a complex overlay of regulations that look at different types of data and industries. I mentioned two types of data – medical and location – that regularly come up in the context of interesting IoT deployments for China. Those are examples of areas where there are specific regulations dealing with the collection and handling of that data in addition to the restrictions found under the data protection and cybersecurity laws.

The regulatory complexity in China goes far beyond data, particularly now with the geopolitical tensions at play. China is obviously a very attractive market, given its scale and how wired its economy has become. For IoT-based businesses there are telecommunications regulations and other areas of regulation to contend with. Given the foreign investment restrictions in force in China, businesses may have to partner



with a domestic Chinese company, forming a joint venture, or deploying some other structural solution to bring their technology and services into the country.

**Q: What about Asia's regulations regarding drones and automotive use cases?**

**A:** Drones and automotive are two very exciting and interesting areas in this part of the world.

We've seen a fairly steady movement toward civil drone regulations. Jurisdictions such as China, Hong Kong, and India have regulations in place that generally have been led by civil aviation authorities with a primary focus on safety and national security rather than on privacy and data protection concerns. We're not yet seeing, for example, cybersecurity or data standards evolving specifically in these jurisdictions in relation to drones.

And we can't ignore the trade issue. Certainly the fact that a number of Chinese manufacturers are leading in this area is raising supply chain and national security issues in the West in the same way that network equipment has. So that's an important point to watch for.

**Q: How important is the IoT to the region's automotive industry?**

**A:** This part of the world – Japan and South Korea, in particular, as well as China – has a number of substantial automotive industry leaders. These jurisdictions are seizing on that strength and looking at the next generation with telematics, self-drives, and other applications. Part of their IoT ambitions is clearly focused on automotive, so there is a big push.

We have other jurisdictions, such as Singapore, that are not leading carmaker jurisdictions but have great technological ambitions. Singapore sees autonomous drive as part of its “smart city” initiative. Singapore has authorized a number of trials and is encouraging R&D and investments in IoT-connected vehicle applications.

**Q: You've said that the rise of industry standards in Asia will be interesting to watch. Why?**

**A:** Because right now, the status quo certainly is very much a patchwork of standards – where standards exist at all, to be frank – and I'll be interested to hear from the other regions as well. We see that various national laws are effectively influencing standards development. China's cybersecurity law is a good example, where technical specifications for information security being developed for network infrastructure are having impacts on IoT.

But apart from that, the field is still open. There has been fairly concerted activity by other jurisdictions that have tried to pave the way for interoperability and set common baselines in areas such as cybersecurity. Japan's General Framework for Secure IoT Systems is a good example, and that's been in play now for a couple of years, although it is a very general and high-level framework.

We note the GSMA has been working with a number of regional operators on developing IoT standards that will support interoperability between and amongst networks. We see government-supported activity in this area in Singapore, Japan, and South Korea in particular – again, jurisdictions that either have an interest in supporting the growth of the technology industry or are exporters of equipment and technologies that are likely to prosper in a more open IoT environment.



**Mark Parsons**

Partner, Hong Kong Office

T +852 2840 50334

mark.parsons@hoganlovells.com

# China issues its fourth draft patent law, after over three years of deliberation

On 4 January 2019, China's National People's Congress (NPC) released draft amendments to the Chinese patent law for public comments (English translation available upon request), proposing, inter alia, higher damages for patent infringement, more options for rewarding inventors under an employee invention remuneration scheme, and patent term extensions for design patents and pharmaceutical patents. The current version of the law, which dates back to 2008, is generally seen as outdated and in need of significant amendment. The fact that this newest draft has been issued after over three years of deliberation, and that it is the fourth iteration of the draft submitted to the NPC, reflects the hotly debated nature of the new provisions of the Patent Law, and the many interests at stake. The draft, if passed, would significantly change China's current patent law. We summarize the highlights below.

## Higher damages for infringement and burden shifting provision

Damages for patent infringement (which, on average, are often considered low by international standards) receive noteworthy attention under the draft. There are three main changes. Firstly, the amount of statutory damages (i.e. lump sum damages granted by a court if the claimant cannot provide sufficient evidence of their actual damages) are significantly raised from a current range of RMB10 000- 1 million to the proposed range of RMB100 000 – 5 million. Secondly, the concept of punitive damages for “serious” wilful infringement is introduced. Under the draft, such severe infringements would be punishable with up to five times the determined amount of damages. Finally, the draft contains a provision allowing for the shifting of the burden of proof for damages in some cases. If the evidence needed to calculate the damages (e.g. accounting books and other materials) is held by the infringer, and the infringer refuses to submit them to the court when ordered to

do so, or submits fabricated evidence, the court can determine the amount of damages based on the initial evidence and calculations of the patent owner and the failure of the infringer to satisfy their burden of supplying contrary evidence. Both the proposed maximum amount of statutory damages (RMB5 million), and the maximum multiplier (5X) for punitive damages are higher than what is currently available under other intellectual property (IP) laws (e.g. RMB3 million and 3X under the trademark law, which was last amended in 2013). Interestingly, even the proposed minimum statutory damages (i.e. RMB100 000) exceeds the average amount of IP damages awarded by Chinese courts in recent years, as reflected in some unofficial data.<sup>66</sup> These changes would be a significant improvement of the current law.

## Patent term extension for pharma patents and design patents

Similar to the legal regimes already existing in the European Union and United States of America, the draft would allow patentees of

innovative pharmaceuticals to apply for a patent term extension of up to five years, to make up for the time spent waiting for regulatory marketing approval. However, an important limitation is that this regime is only available to invention patents for “innovative drugs”, for which marketing approval is simultaneously applied for in China and abroad. Moreover, the total effective term of the patent, after being placed onto the market, cannot exceed 14 years. Also, the new draft makes no mention of the previously proposed patent linkage system, which may be left to be regulated by administrative regulations. Finally, the term of design patents would be extended to 15 years from its filing date, up from 10 years under the current law, and in line with the Hague Agreement Concerning Industrial Designs.

### Inventor compensation

Under the draft, employee inventors or designers may be rewarded in the form of stocks, options, dividends etc. as part of a company policy for promoting employee inventions. The draft remains relatively vague on inventor remuneration and details pertaining to a reasonable invention-creation policy, so it is presumed detailed rules may be left for future implementing regulations.

### E-infringement and network service providers

A new provision in the draft provides that network service providers must comply with infringement notice-and-takedown requests from patent owners or interested parties, when such requests are based on effective court decisions or administrative authority orders, otherwise the network provider will bear joint liability for the online patent infringement.

### Good faith and anti-patent abuse provision

A new article under the draft provides an explicit duty of good faith for both patent applicants and patentees in enforcing their rights. The article moreover unambiguously states that patentees cannot use their patents to exclude or restrict competition. It is possible that this article may form a general legal foundation for the various related standard essential patents (SEP) guidelines issued by the Chinese courts (see for instance here).

### Centralization of administrative enforcement possible

Under the draft, the central, national patent administration department may, at the request of the patentee, handle patent infringement disputes that have “significant influence” throughout the country. Moreover, cases in which the same patent is infringed throughout a region can be combined.

### Attempt to increase patent utilization rate through new open license system

Under the draft, a patentee can register a declaration with the Chinese patent office, stating that it is willing to grant an “open license” to any entity or person that accepts a license under certain specified licensing fees. The Chinese patent office may then decide to publically announce the declaration. During the “open licensing period”, any candidate-licensee could obtain a license under the patent by sending a written notice to the patentee and paying the specified fees, with the caveat that the patentee isn't allowed to grant a sole or exclusive license under the patent during the term of validity of the open license.



**Zhen (Katie) Feng**  
Partner, Shanghai  
T +86 021 6122 3826  
zhen.feng@hoganlovells.com



**Eugene Low**  
Partner, Hong Kong  
T +852 2840 5907  
eugene.low@hoganlovells.com



**Helen Xia**  
Partner, Beijing  
T +86 010 6582 9488  
helen.xia@hoganlovells.com

# References

1. This paper focuses only on Part 1 of the CLOUD Act. Part 2 of the CLOUD Act, which we do not examine, permits the U.S. government to enter into Executive Agreements (“EAs”) with other countries that meet baseline privacy, due process, and human rights standards. The EAs are intended to facilitate streamlined data access for foreign law enforcement authorities in the investigation of serious crimes, provided that they meet baseline privacy, due process, and human rights standards under the CLOUD Act. The CLOUD Act contains certain additional provisions besides Parts 1 and 2. Such provisions are also outside the scope of this paper.
2. Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, §§ 101-106, 132 Stat. 348, 1213-25 (2018).
3. Id. § 103(a)(1), 132 Stat. 1214.
4. For example, the European Parliament issued a nonbinding resolution on July 5, 2018 that calls on the European Commission to suspend the EU- U.S. Privacy Shield unless U.S. authorities can “fully comply” with the framework by September 1, 2018. In particular, the resolution “expresses strong concerns” about the CLOUD Act, which is viewed as having “serious implications for the EU, as it is far-reaching and creates a potential conflict with the EU data protection laws.” Motion for a Resolution, to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) (July 5, 2018), <http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN>.
5. The concept of “control” under U.S. case law relating to criminal and civil procedure is unrelated to the concept of “controller” under the GDPR.
6. See Orin Kerr, A User’s Guide to the Stored Communications Act, 72 Geo. Wash. L. Rev. 1208, 1212 (2004); 18 U.S.C. §§ 2702(a)(3), (b)(2), (c)(1).
7. See, e.g., *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 453 (C.D. Cal. 2007).
8. See Fed. R. Civ. P. 34(a)(1).
9. *United States v. Martin*, No. CR-14-00678-PHX-DGC (D. Ariz. July 21, 2015) (order denying motion to suppress).
10. See *United States v. Warshak*, 631 F.3d 266, 282 (6th Cir. 2010).
11. 18 U.S.C. § 2711(2).
12. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564.
13. *Burrows v. Purchasing Power, LLC*, No. 1:12-CV-22800-UU, 2012 WL 9391827, at \*5 (S.D. Fla. Oct. 18, 2012).
14. *In re Jetblue Airways Corp. Privacy Litigation*, 379 F.Supp.2d 299 (E.D.N.Y. 2005).
15. *United States v. Standefer*, 2007 WL 2301760, at \*5 (S.D. Cal. Aug. 8, 2007).
16. See *Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the “to the public” clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to “any member of the community at large”).
17. *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at \*9 (N.D. Cal. Mar. 26, 2013).
18. 18 U.S.C. § 2510(14).
19. *Kaufman v. Nest Seekers, LLC*, 2006 WL 2807177, at \*6 (S.D.N.Y. 2006) (“An on-line business which provides its customers, as part of its commercial offerings, the means by which the customers may engage in private electronic communications with third-parties may constitute a facility through which electronic communication service is provided.”).
20. See *Walsh Bishop Assocs., Inc. v. O’Brien*, 2012 WL 669069, at \*4-5 (D. Minn. Feb. 28, 2012) (holding that because “[c]ourts interpret the [ECPA/SCA] to encompass internet service providers and telecommunications companies” an architectural firm was not a provider of “electronic communications service” and failed to state a claim under the Act against an employee who accessed information on the firm’s computer system); *Keithly v. Intelius Inc.*, 764 F.Supp.2d 1257, 1271-72 (W.D. Wash. 2011), on reconsideration 2011 WL 2790471 (holding that a company that uses electronic communications services to conduct its business on the internet but does not provide the wire or electronic communications services utilized by its customers was not an internet service provider, a telecommunications company, or a public carrier of any kind, and is therefore was not an “electronic communications service” subject to the protections of the SCA).
21. See, e.g., U.S. Const. amend. XIV.
22. See *In Re Search Warrant No. 16-960-M-1 to Google*, No. 2:16-mj-00960-JS (E.D. Pa. Aug. 17, 2017) (memorandum affirming magistrate judge’s order) (“In manner of operation, then, an SCA warrant is ‘more closely analogous to the workings of subpoenas and court-ordered discovery,’ forms of legal process generally understood to be capable of reaching records in the possession or control of a party of which the enforcing court has personal jurisdiction, regardless of where the records are located, without raising extraterritoriality concerns.”) (internal citation omitted).
23. 18 U.S.C. § 2713.
24. Fed. R. Civ. P. 34(A)(1).
25. As noted above, the concept of “control” discussed in this section should not be confused with the concept of “controller” under the GDPR. The two concepts are different.
26. Jonathan D. Jordan, Out of “Control” Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possessed by a Foreign Parent?, 68 Baylor L. Rev. 189, 200-01 (2016).
27. See, e.g., *In re Subpoena Duces Tecum to Ingeteam, Inc.*, No. 11-MISC-36, 2011 WL 3608407, at \*1 (E.D. Wis. Aug. 16, 2011) (using five factors to measure “whether a subsidiary has ‘control’ over documents held by its foreign parent corporation”); *In re Subpoena to Huawei Techs. Co.*, 720 F. Supp.2d 969, 976 (N.D. Ill. 2010) (using seven factors to measure “the closeness of the relationship between the parties”); *Stella v. LVMH Perfumes & Cosmetics USA, Inc.*, No. 07-CV6509, 2009 WL 780890, at \*2 (N.D. Ill. Mar. 23, 2009) (using four factors to measure “[t]he degree of control, [which] is determined by the ‘closeness of the relationship between the entities’”); *In re Ski Train Fire of Nov. 11, 2000 Kaprun Austria*, No. MDL 1428(SAS)THK, 2006 WL 1328259 (S.D.N.Y. May 16, 2006) (the parent could not shield documents behind a formalistic control analysis when the parent dominated the subsidiary’s board of directors).



28. *United States v. Int'l Union of Petroleum & Indus. Workers*, AFL-CIO, 870 F.2d 1450, 1452 (9th Cir. 1989).
29. *Stream Sicav v. Wang*, 2014 U.S. Dist. LEXIS 81098 (S.D.N.Y. Jun. 12, 2014).
30. *Id.* at \*16.
31. *Id.* at \*15.
32. 18 U.S.C. § 2703(a).
33. *United States v. Perkins*, 850 F.3d 1109, 1119 (9th Cir. 2017).
34. 18 U.S.C. § 2703(b).
35. *Id.* § 2703(d).
36. *Warshak*, 631 F.3d at 288.
37. H.R. Rep. No. 114-528, at 9 (2016).
38. See Dep't of Justice, U.S. Attorneys' Manual §§ 9-13.500-510 (last updated 2018).
39. See 18 U.S.C. § 2518(3)(a) (permitting the approval of wiretap applications only in connection with investigations of certain enumerated crimes).
40. *Id.* § 2518(3)(c) (requiring that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved).
41. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, hereinafter "GDPR".
42. Article 29 Data Protection Working Party, "Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679", WP 253, 3 October 2017, hereinafter "EDPB Guidelines".
43. CJEU, *Rewe-Zentralfinanz eG v. Landwirtschaftskammer*, Case C-33/76, 16 December 1976, point 5.
44. Chapter VII, GDPR.
45. See, e.g., Article 19, Regulation (EU) 995/2010 of the European Parliament and of the Council of 20 October 2010 laying down obligations of operators who place timber and timber products on the market; Directive 2008/99/EC of 19 November 2008 on the protection of the environment through criminal law; Directive 2009/123/EC of 21 October 2009 amending Directive 2005/35/EC on ship-source pollution and on the introduction of penalties for infringement; Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).
46. CJEU, *Commission v Greece*, Case C-68/88, 21 September 1989, point 24.
47. CJEU, *Comet VB v Produktschap voor Siergewassen*, Case C-45/76, 16 December 1976, point 16.
48. *Id.*
49. CJEU, *Ute Reindle v. Bezirkshauptmannschaft Innsbruck*, C-443/13, 13 November 2014, point 39.
50. EDPB Guidelines, p. 7 (bold in the original text).
51. CJEU, *LCL Le Crédit Lyonnais v. Fesih Kalhan*, Case C-565/12, 27 March 2014, point 51.
52. Advocate General Opinion, *Berlusconi and Others*, Joined Cases C-387/02, C-391/02 and C-403/02, 14 October 2014, point 89 (footnotes omitted).
53. European Competition Authorities, ECA Working Group on Sanctions, Pecuniary sanctions imposed on undertakings for infringements of antitrust law, Principles for convergence, May 2008.
54. EDPB Guidelines, p. 6.
55. EDPB Guidelines, p. 11.
56. See *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 3959 (2015); *3.5 GHz Band/Citizens Broadband Radio Service*, FCC.gov, <https://www.fcc.gov/wireless/bureau-divisions/broadband-division/35-ghz-band/35-ghz-band-citizens-broadband-radio> (last visited Mar. 20, 2019).
57. *NE Colorado Cellular, Inc. dba Viaero Wireless*, Kersey, CO, Notice of Violation, File No.: EB-FIELDWR-18-00026229 (rel. Apr. 4, 2018).
58. *NE Colorado Cellular, Inc. dba Viaero Wireless*, Kersey, CO, Notice of Apparent Liability for Forfeiture, File No.: EB-FIELDWR-18-00026229 NAL/Acct No.: 201932030001 FRN: 0001607225 (rel. Feb. 8, 2019).
59. See 47 C.F.R. §§ 1.903; 90.1307.
60. *Id.*
61. See *id.* § 1.80.
62. *Id.*
63. See *supra* note 1 and accompanying text.
64. *Promoting Investment in the 3550-3700 MHz Band*, Report and Order, GN Docket No. 17-258, FCC 18-149 at ¶ 1 (rel. Oct. 24, 2018).
65. See NAL at ¶ 1.
66. See for instance 知识产权损害赔偿认定难,怎么解?and 97%专利侵权案判决采取法定赔偿

# Notes

# Notes

Alicante  
Amsterdam  
Baltimore  
Beijing  
Birmingham  
Boston  
Brussels  
Budapest\*  
Colorado Springs  
Denver  
Dubai  
Dusseldorf  
Frankfurt  
Hamburg  
Hanoi  
Ho Chi Minh City  
Hong Kong  
Houston  
Jakarta\*  
Johannesburg  
London  
Los Angeles  
Louisville  
Luxembourg  
Madrid  
Mexico City  
Miami  
Milan  
Minneapolis  
Monterrey  
Moscow  
Munich  
New York  
Northern Virginia  
Paris  
Perth  
Philadelphia  
Riyadh\*  
Rome  
San Francisco  
Sao Paulo  
Shanghai  
Shanghai FTZ\*  
Silicon Valley  
Singapore  
Sydney  
Tokyo  
Ulaanbaatar\*  
Warsaw  
Washington, D.C.  
Zagreb\*

\*Our associated offices

[www.hoganlovells.com](http://www.hoganlovells.com)

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see [www.hoganlovells.com](http://www.hoganlovells.com).

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2018. All rights reserved. 1059930\_0419