Volume 7, Issue 3, April 2016

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION
2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

How to Protect Your Company's Social Media Currency
Page 2

Clickwrap, Browsewrap and Mixed Media Contracts: A Few Words Can Go a Long Way
Page 4

A Negative Review May Be Protected Activity Under U.S. Employment Law
Page 6

The Internet of Things: Interoperability, Industry Standards & Related IP Licensing Approaches
Page 6

Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement
Page 14

Digital Single Market Strategy Update: Europe Proposes Further Harmonization of Consumer Protection Laws
Page18

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

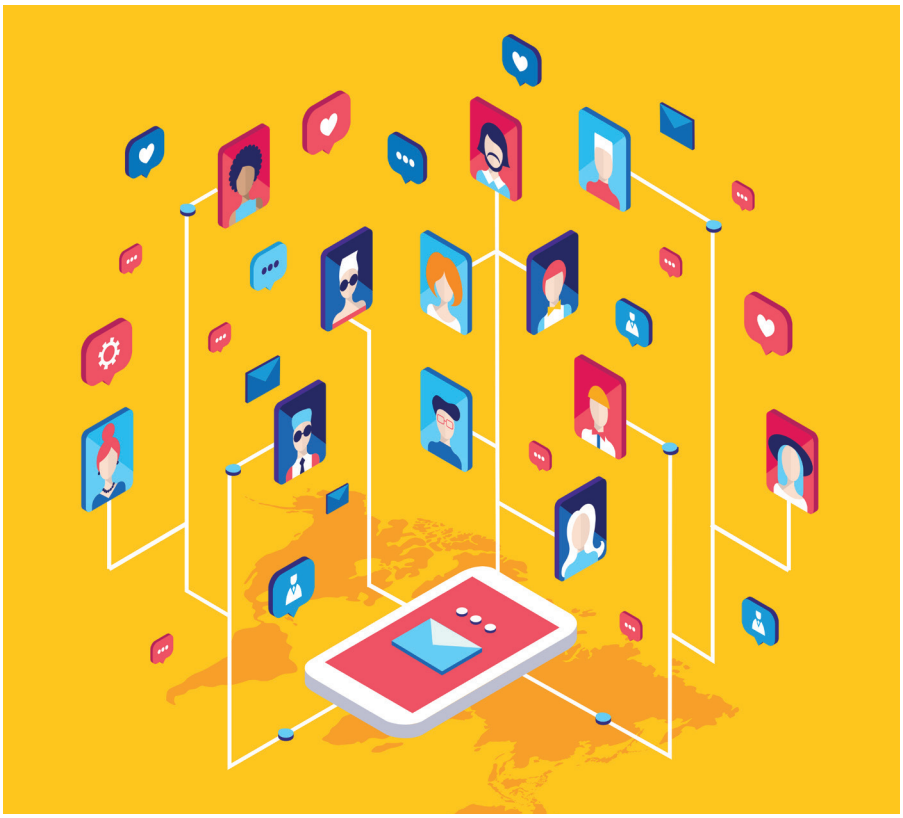
John F. Delaney
Kristina Ehle
J. Alexander Lawrence
Susan McLean
Christine E. Lyon
Sotirios Petrovas
Mary Race
Cynthia J. Rich
Aaron P. Rubin
Stephanie L. Sharron
Joshua R. Stein
Bastian Suurmond
Leanne Ta

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER



Welcome to the newest issue of *Socially Aware*, our Burton Award winning guide to the law and business of social media. In this edition, we discuss what a company can do to help protect the likes, followers, views, tweets and shares that constitute its social media "currency"; we review a federal district court opinion refusing to enforce an arbitration clause included in online terms and conditions referenced in a "wet signature" contract; we highlight the potential legal risks associated with terminating an employee for complaining about her salary on social media; we explore the need for standardization and interoperability in the Internet of Things world; we examine the proposed EU-U.S. Privacy Shield's attempt to satisfy consumers' privacy concerns, the European Court of Justice's legal requirements, and companies' practical considerations; and we take a look at the European Commission's efforts to harmonize the digital sale of goods and content throughout Europe.

All this—plus an infographic illustrating the growing popularity and implications of ad blocking software.

HOW TO PROTECT YOUR COMPANY'S SOCIAL MEDIA CURRENCY

By Aaron P. Rubin and Leanne Ta

Today's companies compete not only for dollars but also for likes, followers, views, tweets, comments and shares. "Social currency," as some researchers call it, is becoming increasingly important, and companies are investing heavily in building their social media fan bases. In some cases, this commitment of time, money and resources has resulted in staggering success. Coca-Cola, for example, has amassed over 96 million likes on its Facebook page, and LEGO's YouTube videos have been played over 2 billion times.

With such impressive statistics, there is no question that a company's social media presence and the associated pages and profiles can be highly valuable business assets, providing an important means for disseminating content and connecting with customers. But how much control does a company really have over these social media assets? What recourse would be available if a social media platform decided to delete a company's page or migrate its fans to another page?

The answer may be not very much. Over the past few years, courts have repeatedly found in favor of social media platforms in a number of cases challenging the platforms' ability to delete or suspend accounts and to remove or relocate user content.

LEGAL SHOW-DOWNS ON SOCIAL MEDIA TAKE-DOWNS

In a recent California case, *Lewis v. YouTube, LLC*, the plaintiff Jan Lewis's account was removed by YouTube due to allegations that she artificially inflated view counts in violation of YouTube's Terms of Service. YouTube eventually restored Lewis's account and videos but not the view counts or comments that her videos had generated prior to the account's suspension.

Lewis sued YouTube for breach of contract, alleging that YouTube had deprived her of her reasonable expectations under the Terms of Service that her channel would be maintained and would continue to reflect the same number of views and comments. She sought damages as well as specific performance to compel YouTube to restore her account to its original condition.

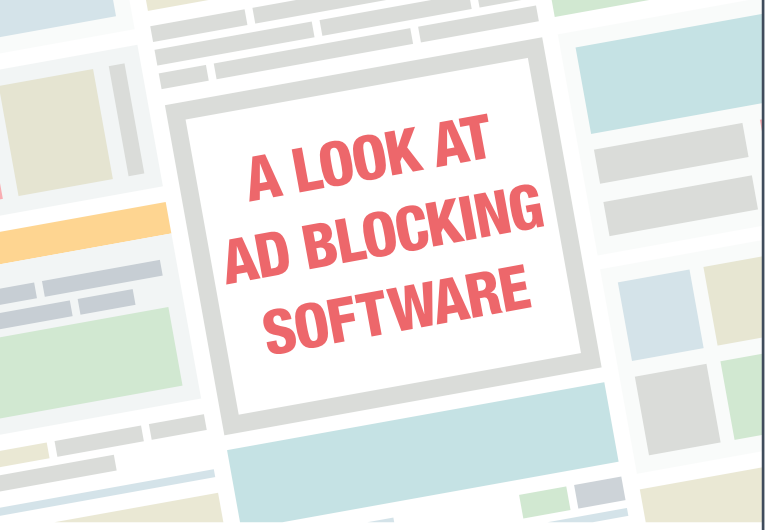
> A good tip is to read the applicable terms of service carefully to understand the platform's rules and the reasons for which a platform may delete or suspend accounts or remove or relocate content.

The court first held that Lewis could not show damages due to the fact that the YouTube Terms of Service contained a limitation of liability provision that disclaimed liability for any omissions relating to content. The court also held that Lewis was not entitled to specific performance because there was nothing in the Terms of Service that required YouTube to maintain particular content or to display view counts or comments. Accordingly, the court affirmed dismissal of Lewis's complaint.

In a similar case, *Darnaa LLC v. Google, Inc.*, Darnaa, a singer, posted a music video on YouTube. Again, due to allegations of view count inflation, YouTube removed and relocated the video to a different URL, disclosing on the original page that the video had been removed for violating its Terms of Service. Darnaa sued for breach of the covenant of good faith and fair dealing, interference with prospective economic advantage and defamation. In an email submitted with the complaint, Darnaa's agent explained that she had launched several large campaigns (each costing $250,000 to $300,000) to promote the video and that the original link was already embedded in thousands of websites and blogs. Darnaa sought damages as well as an injunction to prevent YouTube from removing the video or changing its URL.

The court dismissed all of Darnaa's claims because YouTube's Terms of Service require lawsuits to be filed within one year and Darnaa had filed her case too late. In its discussion, however, the court made several interesting points. In considering whether YouTube's Terms of Service were unconscionable, the court held that, although the terms are by nature a "contract of adhesion," the level of procedural unconscionability was slight, since the plaintiff could have publicized her videos on a different website. Further, in ruling that the terms were not substantively unconscionable, the court pointed out that "[b]ecause YouTube offers its hosting services free of charge, it is reasonable for YouTube to retain broad discretion over [its] services."

Although the court ultimately dismissed Darnaa's claims based on the failure to timely file the suit, the decision was not a complete victory for YouTube. The court granted leave to amend to give Darnaa the opportunity to plead facts showing that she was entitled to equitable tolling of the contractual limitations period. Therefore, the court went on to consider whether Darnaa's allegations were sufficient to state a claim. Among other things, the court held that YouTube's Terms of Service were ambiguous regarding the platform's rights to remove and relocate user videos in its sole discretion. Thus, the court further held that if Darnaa were able to amend the complaint to avoid the consequences of the failure



200 million monthly active users of ad blocking software worldwide.[1]

16% of the U.S. online population blocked ads in the second quarter of 2015.[2]

36.7%
of the online population in Greece blocked ads in the second quarter of 2015, the highest percentage of any European country.[3]

$22 billion
is the estimated amount that ad blockers cost publishers in 2015.[4]

$215 a year
is the estimated ad revenue associated with each U.S. Internet user; as heavy Internet users, those using ad blockers are potentially worth even more.[5]

2%
of Internet users, in return for ad-free access to online information, would be willing to pay a charge equal to the publisher's lost ad revenue.[6]

SOURCES

1. http://www.businessinsider.com/us-publishers-could-band-together-to-stop-ad-blockers-2016-4 (citing survey from research firm Medianomics)
2. http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf
3. http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf
4. https://blog.pagefair.com/2015/ad-blocking-report/
5. http://www.adweek.com/news/technology/how-ad-blocking-could-affect-youtubes-subscription-model-163983 (citing Secret Media)
6. http://www.adweek.com/news/technology/how-ad-blocking-could-affect-youtubes-subscription-model-163983 (citing Secret Media)

to timely file, then the complaint would be sufficient to state a claim for breach of the contractual covenant of good faith and fair dealing.

By contrast, the court found no such ambiguity in *Song Fi v. Google Inc.*, a case with facts similar to those in *Darnaa*. In *Song Fi*, the plaintiff asserted claims for, among other things, breach of contract and breach of the implied covenant of good faith and fair dealing. YouTube raised a defense under the Communications Decency Act (CDA) Section 230(c)(2)(A) which states that no provider of an interactive computer service is liable for removing content that it considers to be obscene, violent, harassing or "otherwise objectionable."

The *Song Fi* court, interpreting this provision narrowly, found that although videos with inflated view counts could be a problem for YouTube, they are not "otherwise objectionable" within the meaning of Section 230(c)(2)(A), and thus, YouTube did not have immunity under that provision. Specifically, the court concluded that, in light of the CDA's history and purpose, the phrase "otherwise objectionable" relates to "potentially offensive material, not simply any materials undesirable to a content provider or user." Further, the requirement that the service provider subjectively finds the blocked or screened material objectionable "does not mean anything or everything YouTube finds subjectively objectionable is within the scope of Section 230(c)." Therefore, the court held that videos with inflated view counts fell outside the statutory safe harbor granted by Section 230(c)(2).

Despite finding Section 230(c)(2) inapplicable, the court ultimately dismissed all of Song Fi's claims. Notably, the court dismissed the contract-based claims with prejudice, holding that, although YouTube's Terms of Service were "inartfully drafted," they "unambiguously" reserved the right for YouTube to remove content in its sole discretion and to discontinue any aspect of its service without liability. Therefore, the court held, the Terms of Service "unambiguously foreclose[d]" Song Fi's claims for breach of contract and breach of the implied covenant of good faith and fair dealing.

Facebook had more luck than did Google in asserting a CDA Section 230 defense in *Sikhs For Justice "SFJ", Inc. v. Facebook, Inc.*, a case brought by a human rights group advocating for Sikh independence in the Indian state of Punjab. Sikhs for Justice (SFJ) alleged that Facebook had blocked its page in India at the behest of the Indian government. SFJ sued in the Northern District of California, asserting several causes of action including race discrimination, and sought damages and injunctive relief.

The *Sikhs for* Justice court ruled in favor of Facebook, citing CDA Section 230(c)(1), which states that "no provider of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Based on this statutory language, Section 230(c)(1) has been interpreted to provide a broad immunity

for website operators against liability arising from user generated content. In dismissing the suit, the *Sikhs for Justice* court explained that the content at issue was provided by SFJ, not by Facebook, and that Facebook's refusal to publish the SFJ page in India was "clearly publisher conduct" that is immunized by Section 230(c)(1).

Notably, the court did not mention the Section 230(c)(2) safe harbor for blocking user content, which YouTube had asserted in SongFi as discussed above. According to some commentators, the *Sikhs for Justice* court's failure to discuss Section 230(c)(2) "highlights its weakness as a safe harbor."

In another case against Facebook, *Young v. Facebook, Inc.*, the plaintiff, Karen Beth Young, found herself suddenly banned from Facebook after sending friend requests to strangers. She sued for breach of the implied covenant of good faith and fair dealing as well as several other claims. In contrast to some of the cases discussed above, the *Young* court found that "it is at least conceivable that arbitrary or bad faith termination of user accounts ... with no explanation at all could implicate the implied covenant of good faith and fair dealing," particularly since Facebook had provided in its Statement of Rights and Responsibilities that users' accounts should not be terminated for reasons other than those described in the Statement. Nonetheless, the court dismissed Young's suit because her complaint did not sufficiently allege that the account termination was undertaken in bad faith or violated Facebook's contractual obligations.

The cases above illustrate how difficult it is for social media users to object to deletion or suspension of accounts or to removal or relocation of content based on a platform's contractual obligations under the applicable terms of service. Users have met with similar obstacles in asserting a property right in social media content.

For example, *Mattocks v. Black Entertainment Television LLC* (which we have discussed previously) involved a dispute between BET and Stacey Mattocks, whom BET had hired to help manage the unofficial Facebook fan page for one of its shows. When Mattocks restricted BET's access to the fan page, BET asked Facebook to "migrate" the fans to another official page that BET had created, and Facebook granted the request. Mattocks sued BET for conversion of her business interest in the Facebook fan page. The court, holding that Mattocks failed to establish that she owned a property interest in the page's likes, granted BET's motion for summary judgment. "If anyone can be deemed to own the 'likes' on a Facebook page," the court stated, "it is the individual users responsible for them." While the *Mattocks* case did not directly target the social media platform itself, it does demonstrate how difficult it can be for a plaintiff to challenge social media platforms' decisions to remove or relocate content based on purported ownership of that content.

SAFEGUARDING YOUR SOCIAL MEDIA CURRENCY

Ultimately, the cases discussed above show that social media platforms have significant control over what is (or isn't) published on their websites, regardless of the amount of time and effort that users have spent building up their individual pages and profiles. With all of this in mind, what can individuals and companies do to protect their social media currency? How can you help ensure that your hard-earned fans, likes, comments and views do not suddenly disappear?

A good tip is to read the applicable terms of service carefully to understand the platform's rules and the reasons for which a platform may delete or suspend accounts or remove or relocate content. Make sure to comply with the platform's rules, including those regarding contests, collection and use of user information and content guidelines. Users should err on the side of caution and avoid posting anything that could be deemed offensive or obscene or that might infringe upon other parties' intellectual property rights. And it goes without saying that users should avoid fraudulent practices, such as artificially driving up view counts or posting fake comments.

Most of all, businesses and individuals should keep in mind that social media platforms have broad discretion when it comes to decisions about what to publish and where. As such, consider spreading your company's social media marketing efforts across a number of different platforms to minimize the impact of sudden content removals or relocations on any one platform. At the end of the day, every social media account—even those with millions of likes or views—is controlled not by the user that created the account but by the platform that hosts it.

CLICKWRAP, BROWSEWRAP AND MIXED MEDIA CONTRACTS: A FEW WORDS CAN GO A LONG WAY

By Joshua Stein and J. Alexander Lawrence

Courts have generally categorized online agreements into two types: "clickwrap" agreements and "browsewrap" agreements.

Clickwrap agreements—which require a user to check a box or click an icon to signify agreement with the terms—are usually enforceable under U.S. law, even where the terms appear in a separate hyperlinked webpage but where language accompanying the box or icon indicates that checking the box or clicking the icon indicates assent to such terms.

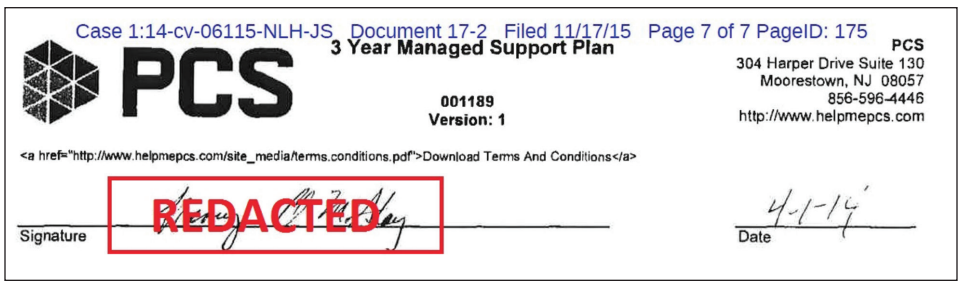
On the other hand, browsewrap agreements—where the terms are passively presented to users in a hyperlink somewhere on a webpage, typically at the

The hyperlink, standing alone, was insufficient to show that Holdbrook had "reasonable knowledge" that the terms and conditions were part of the contract.

very bottom of the page in small font—are often unenforceable because in many cases it cannot be proved the user knew the terms existed or even was aware of the hyperlink.

A New Jersey court recently faced a type of online agreement that did not fit nicely into either category. Where a contract, sent electronically but signed in hard copy, contains a hyperlink to a separate terms and conditions page, are those separate terms incorporated into the agreement? In *Holdbrook Pediatric Dental, LLC, v. Pro Computer Service, LLC*, the New Jersey court said no. A requirement to arbitrate disputes buried in the online terms and conditions page was not incorporated into a contract where the contract merely stated "Download Terms and Conditions" near the signature line.

Again, the signed contract did not itself contain an arbitration clause. Rather, on the last page of the contract, directly above the signature line, the following appeared in small text: " Download Terms and Conditions ," which, if viewed in HTML, would instead appear as "Download Terms and Conditions." The signed contract looked like the below image:


Case 1:14-cv-06115-NLH-JS Document 17-2 Filed 11/17/15 Page 7 of 7 PageID: 175

PCS

3 Year Managed Support Plan

001189
Version: 1

PCS
304 Harper Drive Suite 130
Moorestown, NJ 08057
856-596-4446
http://www.helpmepcs.com

Download Terms And Conditions

REDACTED

Signature

4-1-14

Date

Holdbrook's office manager, Nancy McStay, received the contract in electronic form where the hyperlink was clickable, but then printed and signed a hard copy. PCS argued that because McStay signed the contract, one could assume that she read and agreed to the entire agreement, including the hyperlinked terms and conditions. Holdbrook disagreed. It argued that the contract did not incorporate the terms and conditions for several reasons.

First, the online terms and conditions contained a separate signature block, suggesting that it required additional acceptance, and Holdbrook never signed onto those terms.

Second, Holdbrook claimed that McStay had no idea that additional terms were being incorporated, given the garbled coding of the hyperlink in the printed copy and the fact that the contract contained no clause specifically pointing to the separate terms and conditions.

Applying New Jersey contract law, the court held that "a separate document may be incorporated through a hyperlink, but the traditional standard nonetheless applies: the party to be bound must have had reasonable notice of and manifested assent to the additional terms."

After describing clickwrap and browsewrap agreements, the New Jersey court examined two key cases in this area; *Fteja v. Facebook, Inc.* (which we've discussed previously) and *Swift v. Zynga Game Network, Inc.* In *Fteja*, a New York court found that a user had sufficient notice of Facebook's terms of service even though the terms were only visible to the user during sign-up via hyperlink (like a browsewrap). A notice above the "Sign Up" button stated that "By clicking Sign Up, you are indicating that you have read and agree to the Terms of Service" (like a clickwrap).

Similarly, in *Swift*, a California court found that a hyperlink to the Terms of Service that appeared right below an "Accept" button—along with a statement that clicking "Accept" meant that the user accepted the terms—was sufficient to prove the user agreed to those terms.

The New Jersey court explained that the fact that this case involved "mixed media" did not matter. The contract was "much like the 'clickwrap' agreements in *Fjeta* [sic] and *Swift*, where the 'Terms and Conditions' were contained in a hyperlink immediately next to a mechanism for accepting the agreement. In place of an 'I Accept' icon to be clicked, a Holdbrook representative was required to sign the agreement on paper."

However, the New Jersey court found one crucial component to be missing. In *Fteja, Swift* and other clickwrap cases, a statement draws "the user's attention to the hyperlink" that is "sufficient to provide reasonable notice that assent to the contract included assent to the additional terms." The New Jersey court noted that there was no such statement in this case, nor instructions to sign the contract only if Holdbrook also consented to the additional terms. The hyperlink, standing alone, was insufficient to show that Holdbrook had "reasonable knowledge" that the terms and conditions were part of the contract.

"Further complicating matters" was the fact that the contract was sent in electronic form but could not be accepted in electronic form. It had to be printed and signed. This made it even less clear that the hyperlink contained additional terms.

The New Jersey court noted that discovery might show that Holdbrook actually reviewed the contract electronically, noticed the hyperlink and agreed to its terms. In fact, after conducting some limited discovery, PCS filed a new motion to compel arbitration, which, as of the date of this post, is pending before the court.

Like the courts in *Fteja, Swift* and other clickwrap cases, the New Jersey court took careful note of the language that surrounded the hyperlink to the terms and conditions to determine whether Holdbrook reasonably understood those additional terms were included in the contract. It seems that, for the court, PCS's "Download Terms and Conditions" was just a little too similar to a "browsewrap" agreement to be found enforceable without further inquiry into whether Holdbrook was, in fact, aware of and agreed to the terms.

PCS may have been able to avoid the issue entirely by simply including the following language in the signed agreement: "By signing the agreement, you also accept the Terms and Conditions on the PCS website."

When it comes to enforcing online agreements, a few words can go a long way.

A NEGATIVE REVIEW MAY BE PROTECTED ACTIVITY UNDER U.S. EMPLOYMENT LAW

By Mary Race and Christine E. Lyon

Yelp, Inc. is more accustomed to being on the giving—rather than the receiving—end of a negative review. That changed recently when a Yelp customer service employee, Talia Ben-Ora, posted an open letter to Yelp's CEO on her blog, lamenting her daily struggle to survive in the Bay Area on low pay. Ben-Ora spent much of the letter discussing wages, benefits, and the financial challenges faced by her co-workers:

Every single one of my co-workers is struggling. They're taking side jobs, they're living at home.... Another wrote on those neat whiteboards we've got on every floor begging for help because he was bound to be homeless in two weeks.... Let's talk about those benefits, though. They're great. Except the copays.... Twenty bucks each is pretty neat, if spending twenty dollars didn't determine whether or not you could afford to get to work the next week.

I got paid yesterday ($733.24, bi-weekly) but I have to save as much of that as possible to pay my rent ($1245) for my apartment that's 30 miles away from work because it was the cheapest place I could find that had access to the train, which costs me $5.65 one way to get to work. That's $11.30 a day, by the way. I make $8.15 an hour after taxes.... I woke up today with stomach pains. I made myself a bowl of rice.

...As I said, I spend 80% [of my income on rent]. What do you spend 80% of your income on? I hear your net worth is somewhere between $111 million and $222 million. That's a whole lotta rice.

Shortly after Ben-Ora posted the letter, Yelp terminated her employment. Yelp's CEO stated that her termination was not related to the letter, but Ben-Ora's post has the online world buzzing and Yelp is not receiving positive reviews.

There may be many valid reasons for terminating an employee. Employers should note, however, that the National Relations Labor Board has become increasingly aggressive in protecting an employee's right to discuss wages and working conditions in a public forum, even when that discussion involves disparaging the employer. Under Section 7 of the National Labor Relations Act (NLRA), protesting an employer's labor policies or treatment of employees is considered protected activity, and this protection extends to non-unionized employees as well. While there appear to be no reports of legal claims by Ben-Ora, commentators have raised the question of whether this type of posting might be legally protected under the NLRA.

The National Relations Labor Board has become increasingly aggressive in protecting an employee's right to discuss wages and working conditions in a public forum, even when that discussion involves disparaging the employer.

The Ben-Ora incident is therefore a reminder of the risks employers may face—both legally and from a public relations perspective—in terminating an employee who has recently protested wages on social media.

THE INTERNET OF THINGS: INTEROPERABILITY, INDUSTRY STANDARDS & RELATED IP LICENSING APPROACHES

By Stephanie Lynn Sharron and Nikita A. Tuckett

The financial impact of the Internet of Things on the global economy will be significantly affected by interoperability. A 2015 McKinsey Global Institute report indicated that, "[on] average,

interoperability is necessary to create 40 percent of the potential value that can be generated by the IoT in various settings [...] Interoperability is required to unlock more than $4 trillion per year in potential economic impact for IoT use in 2025, out of a total impact of $11.1 trillion across the nine settings that McKinsey analyzed."

However, at present, there is a lack of consensus between standards organizations and industry stakeholders as to even the most basic technical standards and protocols that apply to how devices communicate. Characterized as a "standards war" between technology groups, companies have competing incentives. While all vendors share an interest in aligned standards that promote IoT development and interoperability, individually some companies seek the perceived competitive and economic advantages of building proprietary systems based on proprietary standards and protocols (or so-called "walled-gardens").

The lack of a uniform standard that applies across devices and networks means that we lack any universally adopted set of semantics. As a result, without clear definition, opportunities for misunderstandings abound. We start then with the definition of two key concepts: the definition of the Internet of Things or IoT, and the definition of interoperability as applied to the Internet of Things.

INTERNET OF THINGS

The term "Internet of Things" is arguably a misnomer in today's rapidly changing technical environment. The term has two components, both of which are somewhat misleading: "Internet" and "things."

The reference to the Internet is misleading because the Internet is not the only networking protocol over which devices communicate. While the Internet is a powerful enabler of the broad adoption of connected devices, the networks and communications protocols that support our connected world are far more diverse and continue to proliferate.

The term "things," while not limiting in and of itself, is vague at best. In this article, when we refer to "things," we intend to encompass all of the types of objects that have the ability to connect and communicate, whether those objects be sensors, computers or everyday things. The ability to connect with other objects and communicate data makes the object "smart."

INTEROPERABILITY

Interoperability is another term that is often articulated as being central to the growth and success of the products and services that leverage the IoT. While interoperability is widely believed to be essential, defining what is meant by interoperability is difficult since interoperability can mean something different when applied to the different parts of the technology stack that comprises the IoT than when applied to the data itself that is communicated and processed through that technology stack.

The European Research Cluster on the Internet of Things has proposed the following definition of interoperability:

"the ability of two or more systems or components to exchange data and use information."

The following definition of interoperability fleshes out some of the concepts that follow in this article.

The ability of objects or devices, whether they be sensors, computers or other everyday things, to connect with each other and communicate data in a form and format that can be understood and processed by other persons or entities and is agnostic as to the hardware or software on which the data is to be further processed and stored.

These definitions are not bulletproof. Rather, they provide fodder for discussion and debate about the extent to which interoperability is desirable within the context of the IoT.

One area of potential confusion in regard to interoperability is distinguishing between the technology and systems required to exchange data from the technology and systems required for the use of that same data. Communications protocols and standards can be leveraged to ensure interoperability across heterogeneous hardware and software systems and platforms. This sort of technical interoperability, however, will not ensure that the data itself that is carried through networked layers of the technology stack are in a form and format that allows for transmission across systems. To support this sort of interoperability, agreed frameworks for syntax and the encoding of data (sometimes referred to as "syntactical interoperability") are needed. Finally, systems will optimally be designed over time that support the ability of users to obtain a common understanding of the information communicated across networked solutions that span diverse geographic and cultural boundaries. This sort of interoperability is referred to as "semantic interoperability." For organizations that use different technology across different cultures in different parts of the world, all three of the above types of interoperability may be desired.

BENEFITS OF INDUSTRY STANDARDS

Standards can offer a number of benefits. Standards can provide assurance to their members that if they implement the standards, their products and services will continue to operate within specified parameters with each other. Technical interoperability is often a goal of industry standards. The broader the set of specified hardware, software and communications protocols a standard supports, the broader the interoperability it may enable.

Choosing to develop in accordance with an industry technical standard can also provide a level of certainty with respect to intellectual property (IP) infringement, albeit not blanket protection. This protection arises because most standards bodies require that participants who contribute to the standard agree to license certain of their IP on pre-defined terms. The scope of the IP rights captured and the terms on which that IP is licensed, however, vary from standard to standard and are based on the participant's level of involvement and contribution. High-level descriptions of the type of license that applies to some of the most well-known IoT standards is included below, to the extent information about the terms is publicly available.

Without coordination as to what options or services products or components that comply with the standard will implement, lack of interoperability will result.

When there is a proliferation of competing standards that cover the same or similar subject matter, however, the standards have the potential to overlap or conflict. Without coordination as to what options or services products or components that comply with the standard will implement, lack of interoperability will result. This has led some industry observers to suggest that broader collaboration between standard-setting organizations, or even consolidation of various IoT standards, could be beneficial in the longer term.

A BUSINESS CASE FOR INTEROPERABILITY

Despite these early movements, whether and the extent to which the various standards bodies will coordinate or consolidate is an open point. Some question whether such consolidation is necessary or even feasible, because interoperability takes place at different layers within the communications protocol stack among IoT systems and devices. Others emphasize that true interoperability requires any IoT device to be able to speak the same language, and connect and share information with other devices and systems, irrespective of platform or operating system (OS), and that this requires one de facto protocol.

The time and investment required by industry stakeholders to participate in a range of standardization efforts is significant, but there is likely to be overlap and even conflicts between some of the standardization protocols. The lack of a collaborative effort to produce a uniform standard could produce conflicting protocols, delay product development and prompt fragmentation across IoT products and services. Such a fragmented array of proprietary IoT technical standards will impede value for users and industry.

Central challenges raised by the proliferation of IoT interoperability standards include the following:

- Device manufacturers perceive a market advantage in establishing a proprietary ecosystem of compatible IoT products that limit interoperability to those devices within the manufacturer's product line. By maintaining the proprietary nature of these systems, developers exert more control over the user experience. These "walled gardens" are opposed by interoperability supporters as impediments to user choice because they arguably deter users from changing to alternative products. Some also argue that they create impediments to innovation and competition, limiting competitors' ability to develop new products compatible with the standardized infrastructure.

- One of IoT's primary attractions is the ability of connected devices to transmit and receive data to and from cloud services, which in turn may perform powerful analytic functions. The lack of a consistent, platform and OS-agnostic standard governing the collection, processing and sharing of such data may inhibit the ability of users to access the originating data, move to other service providers or perform their own analyses.

- The lack of an existing and proven standard that IoT device manufacturers may use to assess technical design risks in the development process increases development costs.

- In the absence of standardization, developers face the behemoth task of developing integrations with legacy systems, and end users will be faced with the challenge of configuring multiple individual devices across a range of standards. In addition, product developers may be dissuaded from developing new products due to uncertainty as to compliance with future standards.

- End users may be discouraged from purchasing products where there is integration inflexibility, configuration complexity or concern over vendor lock-in, or where they fear products may be obsolete due to changing standards. The complications posed by a lack of uniform connectivity standards for product development and industry growth are evident in the competing, incompatible standards for devices with a low-range and medium-to-

low data rate (i.e., ZigBee, Bluetooth and LTE Category 0).

- Lack of reference and architectural models that take into account the various needs for interoperability and standardization may also have adverse consequences for the networks with which IoT devices connect, since poorly designed sensor networks may use disproportionate bandwidth and be greedy consumers of available power.

In contrast, well-defined device interoperability standards may encourage innovation as disruptive technologies emerge, provide efficiencies for IoT device manufacturers and generate economic value as "things" become cheaper, smarter and easier to use. Barriers to entry may be lowered. Moreover, interoperability facilitates the ability of users to select the devices best suited to the user's needs in an environment where different devices can share and communicate data between each other. Nevertheless, such arguments remain counterbalanced by companies' perceived competitive and economic advantages of building proprietary systems for market domination in the IoT.

THE IOT STANDARDS SMORGASBOARD

IoT standards, including those that adopt protocols that specify communication details for IoT devices, are central to the interoperability discussion for the IoT. A number of standards bodies, consortiums and alliances are currently working on IoT standards issues. Below is a non-exhaustive list of some of the current major players in the development of standards, the covered products and services and the licensing approaches that apply to the IP that is used by products and services that implement these standards.

Standards that offer limited protection from infringement of the IP rights of their contributors can lead to legal and business uncertainty. Legal uncertainty can arise because of the lawsuits for infringement that may be brought by contributors who have promoted the adoption of features or works into the standard that if used without a license, would infringe their patents or copyrights. There may be business uncertainty because companies lack predictability regarding what the ultimate cost of implementation of the standard may be should contributors charge for licenses to IP required to implement the standard.

Central to this debate is what the appropriate licensing terms should be for contributors to a particular standard. As seen in the telecommunications industry, standardized licensing terms can affect the way an industry evolves: licensing terms that are overly aggressive or demand too much of a participant will be eschewed in favor of more acceptable models. This alert examines the fragmented environment of IoT technical standards and analyzes the differences between the proposed licensing models, exemplifying how various standard bodies are attempting to reconcile the issue.

Open Interconnect Consortium

Standard
IoTivity

The Open Interconnect Consortium (**OIC**) launched in July 2014, backed by such vendors as Intel, Samsung Electronics, Cisco, GE Software, Atmel, Dell, Honeywell, IBM, Mediatek, ZTE, Acer, Broadcom, Asus, National Instruments and many others. The OIC's stated focus is "defining a common communications framework based on industry standard technologies to wirelessly connect and intelligently manage the flow of information among personal computing and emerging IoT devices, regardless of form factor, OS, or service provider."

History, Scope and Members
In early 2015, the OIC released a specification called IoTivity, an open source framework implementing the OIC Standards for device-to-device connectivity. Operating on a constrained application protocol (CoAP), IoTivity has limited platform support, but is focused on security, simplicity and rapid development. The OIC's open source standards cover device discovery, communication, data exchange and other functions in multiple domains, including home automation, automotive, enterprise, health care and industrial scenarios, with an initial focus on smart home and office solutions.

License Approach
Under the OIC's Intellectual Property Rights Policy, the OIC's licensing policies contain a "**RAND-Z**" (or "**FRAND**") provision that requires participating companies to offer a zero-royalty, reasonable and non-discriminatory license to their code for member organizations. In addition, each member must agree that it will not seek to enforce its IP rights against another member if reasonable and non-discriminatory compensation ("**RAND**") for practice of IP rights can otherwise be obtained. Further, each member *and its affiliates* must grant the OIC a worldwide, irrevocable, non-exclusive, non-transferable, sublicensable, royalty-free copyright license to reproduce, create derivatives of, distribute, display, perform and edit the member's contributions for the purposes of developing, publishing and distributing: the final specifications; products incorporating compliant portions based on the specifications; and submissions to an approved standards development organization. Subject to the member's retention of its copyright in the individual contribution, OIC owns all rights in the compilation

of contributions forming the final specifications and related works. Code contributions under the reference implementation, IoTivity, are licensed under the Apache 2.0 license.

AllSeen Alliance

Standard
AllJoyn

History, Scope and Members
Launched in December 2013, AllJoyn is an open-source software system intended to enable compatible smart devices, irrespective of OS and network protocols, to find and coordinate with each other. The project was developed by Qualcomm Innovation Center and is now a collaborative open source project of the AllSeen Alliance. Members of the Alliance include Qualcomm, The Linux Foundation, Cisco Systems, Arcelik A.S., Canon, Electrolux, Haier, LG, Microsoft, Panasonic, Philips, Qeo, Sharp, Silicon Image, Sony, Asus, AT&T, Cisco, Honeywell, HTC, IBM, Lenovo, Symantec, TrendMicro, Vodafone and many others.

The open source AllJoyn protocol enables device manufacturers to create custom apps for integrating devices onto a Wi-Fi network. Products that use AllJoyn include Panasonic's multi-room audio systems and LG's smart TVs; in November 2014, Microsoft announced it was building the AllJoyn framework into Windows 10. In early January 2016, the AllSeen Alliance announced its first update to the AllJoyn Gateway Agent Plan, originally released on April 19, 2015. This extension of the AllJoyn framework provides a standard and secure method to remotely access and manage IoT devices and applications via external/cloud networks and the Internet. This moves the IoT from a series of Internet-connected gadgets into a manageable system.

License Approach
Unlike the OIC, AllJoyn does not contain a RAND-Z licensing term—a key difference between the organizations. Members of the AllSeen Alliance and all non-members that contribute to the Alliance must pledge not to bring a claim of infringement of the contributor's pledged patent claims against any entity that uses, sells, offers for sale, leases, licenses, imports, distributes or otherwise exploits an official code release by the Alliance that meets the Alliance's certification requirements. Pledged patent claims are those that are directly infringed by the use, sale or other disposition of the code that is contributed by the contributor alone and not in combination with any other contribution. The agreement does not extend to contributions made by others, any modification of the contributor's contribution or combination of the contributor's contribution with anything else. This addition to the Alliance's patent policy was introduced in January 2015; previously, AllSeen's IP policies had covered only copyright. Code released by the Alliance for the AllJoyn framework is licensed to users under the ISC License, which grants permission to use, copy, modify and/or distribute the software for any purpose with or without fee, provided that a copyright notice appears in all copies. Contributors are required to enter into a Contributor Agreement pursuant to which contributors can elect either to assign to the Alliance the copyright rights and interests in the contribution subject to a license back to exploit the work, or to grant to the Alliance a non-exclusive, broad copyright license.

Thread Group

Standard
Thread

History, Scope and Members
Thread Group's "Thread," an IP-based wireless networking protocol, is an initiative launched by Google's Nest Labs, Samsung Electronics, ARM Holdings, Freescale Semiconductor, Silicon Labs, Big Ass Fans and Yale Locks & Hardware.

Thread relies on a low-power radio protocol called IPv6 over Low Power Wireless Personal Area Networks ("6LowPAN"). Unlike Wi-Fi, which sends large quantities of data and consumes large amounts of power, Thread sends small amounts of data and consumes very little power. The protocol gives each device an IPv6 address and utilizes mesh networks that scale to hundreds of devices without a single point of failure (i.e., without the need for a hub device), and involve "banking-class" encryption. According to Thread Group, as the technology only defines networking, in theory, high-layer standards such as AllJoyn or IoTivity, which still utilize Wi-Fi or Bluetooth networks, could be used in Thread-enabled products.

License Approach
Like OIC, patents that are necessarily infringed by required portions of the final Thread specification are licensed on a perpetual, royalty-free basis ("**RAND-RF**"). Each participant must grant the Group and each participant a worldwide, irrevocable, non-exclusive, non-transferable, royalty-free copyright license to reproduce, create derivative works of, distribute, display and perform (with the right to sublicense) each final Thread specification for the purposes of developing, publishing and distributing the final specification and related materials, as well as for promotional materials. Subject to each member's retention of the copyright in its individual contribution, each member must convey to the Group a non-exclusive, undivided and equal ownership interest in any copyrights contributed to the final Thread specification, deemed "ownership of a collective work" under 17 USC 201(c). This copyright license survives any withdrawal from membership of the granting participant from the Thread Group.

ZigBee Alliance

Standard
ZigBee

History, Scope and Members
Established in 2002, the ZigBee Alliance is a non-profit association of 452 members, including ARM, Belkin, AT&T, Bosch, Broadcom, Cisco Systems, Emerson, Huawei and many others.

The ZigBee Alliance's standard, ZigBee, is a common wireless language that everyday devices utilize to connect to one another. In December 2015, the ZigBee Alliance announced that its members had ratified the ZigBee 3.0 specification, which includes a common application library that unifies the various application-specific versions of its wireless specification into a single standard. Millions of ZigBee-enabled products exist on the market today, including in smart homes, connected lighting, and the utility industry.

License Approach
Under the ZigBee Alliance's Intellectual Property Rights Policy, each ZigBee standard is made available on a RAND basis: each contributing member must grant to each other member a non-exclusive license without a right to sublicense, to make, have made, use, import, sell, offer to sell, license, promote or otherwise dispose of the resulting product or technology. The license is granted only under claims of the contributor's patents that cover or directly relate to one or more of the specifications if: (1) the patent claim is necessarily infringed by the specification, (2) no commercially reasonable non-infringing implementation of the specification exists, and (3) such infringement is necessary to meet the implementation requirements of the specifications. The Alliance charges no royalty for any use of the standards, and RAND terms are available to members and non-members.

AVnu Alliance

Standard
AVB/TSN

History, Scope and Members
Launched in August 2009 by founding members that included Broadcom, Cisco Systems and Intel, the AVnu Alliance is a consortium of automotive and consumer electronics companies collaborating to establish and certify the interoperability of open Audio Video Bridging (AVB) standards.

The Alliance focuses on "creating an interoperable ecosystem servicing the precise timing and low latency requirements of diverse applications using open standards through certification."

License Approach
Under the AVnu Alliance Intellectual Property Rights Policy, when a member or its affiliates make a contribution to a specification, the member and its affiliates must grant to other participants and their affiliates, on a RAND basis, a non-exclusive, non-transferable, non-sublicensable, irrevocable worldwide license (with or without compensation at the member and its affiliates' option) under certain of its patent claims that are necessarily infringed by compliance with the final specification and that are within a specified "scope" limited to functionality that enables products to interoperate, interconnect or communicate. The license grants the right to make, have made, use, import, offer to sell, lease, sell and otherwise distribute only those portions of products that implement and are compliant with the relevant portions of the final specification and are within the bounds of the above "scope." The Intellectual Property Rights Policy also contains a broad license grant by members with respect to the member's copyrights in any contributed materials. A range of AVnu-certified products are available across automotive, consumer and industrial electronics markets.

Industrial Internet Consortium

History, Scope and Members
Founded in March 2014 by General Electric, Cisco Systems, IBM, Intel and AT&T, the Industrial Internet Consortium (**IIC**) focuses on industrial applications of the IoT and "setting the architectural framework for the industrial internet." The IIC has grown to more than 100 members, including Microsoft, Samsung and Huawei Technologies.

The IIC reports that it will not develop a set of standards but will work with standards bodies to ensure technologies work together across business sectors and to identify, assemble and promote best practices. In particular, the IIC wants to encourage coordination among industries within which IoT and the older machine-to-machine (**M2M**) technologies have been developed in relative isolation. That will involve defining requirements for standards, designing reference architectures and frameworks necessary for interoperability, and creating new industry cases and testbeds for real-world applications.

License Approach
The IIC's intellectual property policy incorporates a broad copyright license, but unlike many of the other standards initiatives, lacks any policy with respect to the grant of rights under contributor patents that may be infringed by their contributions. This may be in part due to the fact that the IIC is not establishing a standard itself, but rather working to encourage coordination across standards.

OneM2M

Standard
OneM2M

History, Scope and Members
Established in July 2012 by a consortium of ICT standards development bodies, OneM2M is a standard that provides a common M2M

service layer that can be embedded within various hardware and software to connect IoT devices. The partnership currently has 216 participating partners and members, including Alcatel-Lucent, Adobe, AT&T, BT, Cisco, Ericsson, Deutsche Telekom, IBM, Intel, Samsung, Sierra Wireless and Telefonica. OneM2M has two types of members: Partner Type 1 comprises membership organizations themselves, and Partner Type 2 comprises members who are also participants in a Partner Type 1 organization or have otherwise had their IPR policies vetted by OneM2M at the time they joined. Ultimately, each partner must have agreed to an IPR policy that is compliant with the OneM2M IPR principles.

License Approach
OneM2M's partnership agreement states that the copyright in technical specifications and reports are jointly owned by the Type 1 partners. Trademark usage is left to agreement among the Type 1 partners. With respect to patents, the organization's IPR principles state that members must comply with a FRAND IP rights licensing regime.

Wi-Fi Alliance

Standard
Wi-Fi HaLow

History, Scope and Members
In early January 2016, the Wi-Fi Alliance announced its new IoT specification, Wi-Fi HaLow, based on the pending IEEE 802.11ah specification, which is claimed to double the distance and cut the power consumption of traditional Wi-Fi. The Wi-Fi Alliance, which has about 700 vendors as members, expects to launch a certification process for Wi-Fi HaLow products in 2018; however, it is anticipated that products supporting the Wi-Fi HaLow specification will enter the market earlier.

License Approach
The IEEE requires IEEE members to license patents to users of the IEEE standards on FRAND terms. The IEEE IPR policy requires the licensing of patent claims, the practice of which is necessary to implement either mandatory or optional portions of the standard when. if at the time of the standard's approval, there was no commercially and technically feasible non-infringing alternative means of implementation. The rights extend to any Compliant Implementation, which is defined as any product (including any component, sub-assembly or end product) or service that conforms to any mandatory or optional portion of a normative clause of an IEEE standard. In early 2015, in a hotly debated move, the IEEE amended its IP policy to clarify that members may charge a reasonable royalty that is based in part on the value that the functionality of the claimed invention or feature within the essential patent claim contributes to "*the smallest saleable Compliant Implementation*" that practices the essential patent claim.

IEEE

Standard
IEEE P2413

History, Scope and Members
The Institute of Electrical and Electronics Engineers (**IEEE**) project P2413 serves as a reference architecture incorporating more than 350 IEEE standards applicable to IoT, and more than 110 new IoT-related standards in various stages of development. P2413 is intended to define the "basic architectural building blocks and their ability to be integrated into multi-tiered systems." Among other things, project P2413 plans to turn the information from different IoT platforms into commonly understood data objects. The group held its first meeting in July 2014, with 23 vendors and organizations involved, and hopes to finish its work on the future standard by 2016. See the discussion of Wi-Fi HaLow for the IEEE's IP licensing approach.

License Approach
Not publicly available.

ITU-T

Standard
ITU-T SG20

History, Scope and Members

In June 2015, Study Group 20 of the International Telecommunication Union announced its work developing standardization requirements for IoT technologies, with an initial focus on IoT applications in smart cities and communities. The SG20 standard is focused on developing "international standards to enable the coordinated development of IoT technologies, including M2M communications and ubiquitous sensor networks."

License Approach
The ITU-T publishes a Common Patent Policy that describes a code of practice with respect to patents. Disclosure of known patents and patent applications (whether their own or third-party patent rights) by parties participating in the ITU is required. While in general the detailed arrangements with respect to patent licensing are left to the parties to negotiate, if a patent is disclosed with respect to a recommendation or deliverable of the ITU-T, and a patent holder is not willing to negotiate a FRAND license (whether royalty-free or royalty-bearing), then "the Recommendation or Deliverable will not include provisions depending on the patent."

Google

Standard
Brillo & Weave

History, Scope and Members
In May 2015, at Google's I/O 2015, Google announced Brillo and Weave. Brillo, an IoT OS that consists of an Android-based OS, core platform services and a developer kit, links IoT devices with each other, with other devices and with the cloud. Brillo uses Google's communications protocol, Weave, the standard that Google hopes to promote as the default standard for all IoT devices. Weave is

a cross-platform protocol that enables device setup from a mobile phone, communication between devices and to the cloud, and user interaction from mobile devices and the web. Weave is operating system-agnostic, will work with Brillo but also with other operating systems, and will work on top of a variety of radio technologies (i.e., Thread, ZigBee, Bluetooth, and Wi-Fi). In August 2015, Google disclosed its product Google OnHub, the first Brillo-enabled device for the smart home. Intel announced that its Intel® Edison computer module is one of the first platforms to support Brillo.

License Approach
Not publicly available.

Z-Wave Alliance

Standard
Z-Wave

History, Scope and Members
Established in 2005, the Z-Wave Alliance's standard, Z-Wave, is a low-powered radio frequency communications technology that supports full mesh networks without the need for a coordinator node. The Z-Wave Alliance has over 375 members, and Z-Wave–powered products and applications cover a range of control and monitoring for residential and light commercial environments. The Z-Wave Alliance's stated goal is to "to bring advanced, yet practical wireless products and services to market that work together seamlessly, regardless of brand or vendor." According to the Z-Wave website, there are over 1,400 Z-Wave interoperable products available, and over 40 million Z-Wave products worldwide. The technology is licensed by Sigma Designs under a Z-Wave Technology License Agreement, the terms of which are not publicly available.

License Approach
Not publicly available.

OUR WAY OR THE HIGHWAY?

Disagreement over the appropriate IP licensing terms for each of the proposed standards has characterized the standards debate to date. In October 2014, Broadcom, a founding member of the OIC, reportedly quit the group due to a disagreement over the IP licensing terms that required companies contributing code to the project to waive their right to assert their donated IP against infringers. In contrast, at the time, the AllSeen Alliance did not have such a provision, but the Alliance's IP Policy was amended in January 2015 to include a comparable non-assert provision, seemingly rendering the dispute moot.

Will these standard-setting organizations learn from the historical experience in other sectors regarding standard-essential patents (**SEPs**) and FRAND licensing terms? The problem is as follows: for IoT to operate in a seamless and interoperable way, standardized technology is essential. If the standardized elements of such technology are patented, this creates a barrier to entry to the IoT. Without a license, third-party users may be forced to either infringe upon such patents or pay exorbitant license fees. Other technology industries, such as the smartphone industry, have required owners of SEPs to offer non-exclusive licenses to prospective licensees on FRAND licensing terms to mitigate this issue.

However, the process for agreeing to FRAND terms is seldom straightforward. Parties may not agree to what constitutes "fair and reasonable" in the context of IoT licenses, particularly given the prospect of enormous growth in the industry. Therefore, although many of the standards bodies above have adopted RAND or FRAND licensing models, the determination of what those RAND terms should be across the industry is far from settled.

Which standards will ultimately garner the widest adoption also remains unclear. Companies like Qualcomm and Intel have joined many of the standards organizations instead of backing a single one. Nonetheless, there have been recent movements by key players toward a more collaborative effort. In April 2015, the ZigBee Alliance and the Thread Group announced a collaboration to allow the ZigBee Cluster Library to run over Thread networks, representing one of the first steps toward interoperability in the fragmented IoT space. Qualcomm announced in July 2015 that it would join the Thread Group as a member of the board, opening the door for potential cooperation and collaboration between multiple bodies of which it is a member. In November 2015, the OIC announced that it had acquired the assets of the UPnP (Universal Plug and Play) Forum, which had been working on network connectivity since 1999. Earlier in 2015, the IIC and OIC announced a strategic liaison, including sharing use cases and architecture requirements, to "accelerate the delivery of an industrial grade communications framework for the IoT." Further, in December 2015, the ZigBee Alliance announced that it was working with EnOcean Alliance, a consortium for battery-less, wireless smart buildings and smart homes, to combine the benefits of EnOcean energy harvesting wireless solutions with ZigBee 3.0 for worldwide applications in self-powered IoT sensor solutions.

CONCLUSIONS

Technical and legal uncertainty, if left unchecked, can threaten to slow the maturation and growth of the technologies that the standards are intended to promote, as well as the businesses whose operations, products and services depend on the interoperability achieved through implementation of the standards. While it may seem that interests should align to create more certainty with respect to both technical and legal risks, this is not always the case. Barriers to entry can protect companies against competition and benefit those companies with the resources to understand and adapt to these risks. For many companies, however, the lack of harmonization can present substantial if not insurmountable obstacles.

For the IoT to achieve its potential for enhanced interoperability, adoption of standards and licensing practices that reduce technical and legal uncertainty are required so that information generated by smart devices may be shared across platforms to create new and innovative functionality. The myriad standards that define the wider framework of IoT interconnection are paradoxically competing to be the most open and most interoperable. As the IoT develops, networks of standardized technology (and the range of standards governing them) will continue to proliferate. Whether the IoT industry will move toward collaborating to achieve broader interoperability and adopting licensing terms that reduce IP risk likely will influence the extent to which the full potential for IoT will be achieved and how quickly emerging IoT technologies will mature and be adopted.

PRIVACY SHIELD VS. SAFE HARBOR: A DIFFERENT NAME FOR AN IMPROVED AGREEMENT?

By Sotirios Petrovas, Cynthia J. Rich and Bastiaan Suurmond

The European Commission (the "Commission") and the U.S. Department of Commerce issued the draft legal texts for the much anticipated EU-U.S. Privacy Shield (the "Shield"), set to replace the currently inoperative Safe Harbor program ("Safe Harbor"). The new agreement is aimed at restoring the trust of individuals in the transatlantic partnership and the digital economy, and putting an end to months of compliance concerns of U.S. and EU companies alike. The draft will be discussed with EU data protection authorities (DPAs) and adopted by Member States representatives before it becomes binding.

The publication of the Shield documents, on February 29, 2015, came at a time of high expectations and a certain tension. Last October, the European Court of Justice (the ECJ) invalidated the Commission's decision 2000/520/EC and effectively shut down the Safe Harbor framework, which had previously allowed thousands of European companies to send personal information to U.S. companies that had committed to protecting personal information. As a result, thousands of U.S. and EU companies were suddenly left in a legal limbo. In response to the risk of enforcement against companies relying on Safe Harbor, and to address the concerns raised by EU DPAs, the Commission announced in early February that a new political agreement had been reached with the U.S. government. It also made good on its promise to make the details of the agreement public by month's end.

At first glance, the Shield bears a strong resemblance to Safe Harbor, which misled some commentators to denounce it as a mere duplicate in disguise. However, the Shield introduces substantial changes for data protection, including additional rights for EU individuals, stricter compliance requirements for U.S. organizations, and further limitations on government access to personal data. From the perspective of U.S. companies, it appears that the Shield may actually signify a shift to heavily monitored compliance. In this sense, the question may no longer be "How good is the Privacy Shield for privacy?" but rather "How burdensome will it become for businesses?"

This alert takes a closer look at the Shield and highlights some of the key differences from the Safe Harbor and other available data transfer mechanisms.

Some of the key takeaways include:

- Safeguards related to intelligence activities will extend to all data transferred to the U.S., regardless of the transfer mechanism used.
- The Shield's dispute resolution framework provides multiple avenues for individuals to lodge complaints, more than those available under the Safe Harbor or alternative transfer mechanisms such as Standard Contractual Clauses or Binding Corporate Rules.

Before settling on a transfer mechanism, organizations will want to consider the regulatory involvement and compliance costs associated with each option.

- An organization's compliance with the Shield will be directly and indirectly monitored by a wider array of authorities in the U.S. and the EU, possibly increasing regulatory risks and compliance costs for participating organizations.
- The Department of Commerce will significantly expand its role in monitoring and supervising compliance, including by carrying out *ex officio* compliance reviews and investigations of participating organizations.
- Participating organizations will be subjected to additional compliance and reporting obligations, some of which will continue even after they withdraw from the Shield.

OVERVIEW

The Commission made public all the documents that will constitute the new agreement, namely: a draft Adequacy Decision, FAQs, a Factsheet,

Annexes detailing the principles and various compliance mechanisms and a Commission Communication describing the current developments in the broader context of transatlantic discussions of the past few years.

In its press release, the Commission stated that the Shield "reflects the requirements" set by the ECJ in its ruling from October 6, 2015 (the "*Schrems* ruling"). Key concerns of the *Schrems* ruling included: (1) the indiscriminate and excessive government access to EU citizens' personal information, and (2) the lack of judicial redress mechanisms for EU citizens for privacy related complaints.

According to the Commission, the Shield will provide for "strong obligations on US companies" as well as "robust enforcement" mechanisms to ensure that such obligations are complied with. It will lay down "clear safeguards and transparency obligations on US government access." Thirdly, it will ensure effective redress of EU Citizens' rights by means of "several redress possibilities." Finally, an annual joint review mechanism will allow the Commission, the U.S. Department of Commerce, and the European DPAs to monitor how well the Shield functions.

ASSESSMENT OF KEY ASPECTS

The following is a discussion of several key aspects of the new agreement, in relation not only to its predecessor, Safe Harbor, but also to other available data transfer mechanisms such as Binding Corporate Rules ("BCRs") and EU Standard Contractual Clauses ("SCCs").

1. Transfers to Third Parties

One of the important changes pertains to conditions for participating organizations to transfer the data to third parties. Under the Safe Harbor principles, an organization had to provide notice and choice prior to disclosing personal information to a third-party controller. This was not required if the third party was "acting as an agent to perform task(s) on behalf of and under the instructions of the organization" (i.e., the processor) (See *Onward Transfer* principle, Safe Harbor Decision 2000/520/EC, Annex I). For sharing data with an agent, the organization was required to:

- "ascertain that the third party certified to Safe Harbor principles or another adequacy finding;" or
- enter into a "written agreement requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles."

Under the Shield principles, the rules for transfers to third-party controllers and agents change considerably. According to the Third principle (*Accountability for Onward Transfer*), to make transfers to "agents" (or "processors"), organizations must meet a host of requirements, including complying with the principle of purpose limitation, ensuring that the agent provides the same level of protection as required by the Shield's principles, and stopping and remediating unauthorized processing. Also, more significantly, organizations must provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request. While the obligation to provide a copy of privacy provisions also exists under SCCs (Controller-to-Processor), there the obligation for the U.S. company (the data importer) is limited to providing copies of sub-processing agreements to the data subject (the individual) or the data exporter (the EU company), not directly to a supervisory authority.

Moreover, notwithstanding having met these requirements, the organization *remains liable* if its agent processes the personal information in a manner inconsistent with the Shield principles, *unless it proves that it is not responsible* for the event giving rise to the damage (Principle 7(d), *Recourse, Enforcement and Liability*). This reversal of the burden of proof will mean that companies face a challenge in practice to show that they are not liable for their agents' violations, even if the agent acted in contravention with its contractual obligations.

For onward transfers to controllers, the Shield principles add a new requirement to the notice and choice obligations that existed under the Safe Harbor. Now, organizations will be required to enter into a contract that provides that the data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipients will provide the same level of protection as the Shield principles. Some limited exceptions are provided for occasional employment-related operational needs, however. Here, too, the Shield goes beyond what is required under the SCCs (Controller-to-Controller), where the U.S. company (data importer) has to address the cross-border transfer. The individual's right to object (as opposed to consent) is only one of the means to legitimize the transfer to third-party controllers, not a prerequisite for all transfers.

However, for transfers to affiliated companies, the Shield principles provide a bit more flexibility than the SCCs, namely that a contract is not always required: data controllers within a "controlled group of corporations or entities" may base such transfers on other instruments, such as BCRs or other intra-group instruments (e.g., compliance and control programs), ensuring the continuity of protection of personal information under the Shield principles. The participating organization remains responsible for compliance with Shield principles.

2. Safeguards Related to Intelligence Activities Will Extend to All Data Transferred to the U.S.

In early February, the Commission indicated that the U.S. has given written assurances that access to EU citizens'

personal data by the U.S. government will be subject to "clear limitations, safeguards and oversight mechanisms" and that any exceptions will be "necessary and proportionate." Also, an Ombudsman within the Department of State will be responsible for receiving and investigating complaints and inquiries about U.S. intelligence practices from EU individuals. The Ombudsman will, however, have no independent investigative or enforcement powers.

Until now, it was unclear whether such safeguards would be confined to data transferred via the Shield or if they would also apply to all data irrespective of the transfer mechanism used. In the context of the WP29 discussions on the consequences of the *Schrems* ruling on other transfer mechanisms, the concern was that European DPAs might decide to suspend transfers to the U.S. based on SCCs or BCRs because of mass and indiscriminate surveillance and excessive access to such data by the U.S. government.

From the documents made public on February 29, it appears that U.S. commitments will extend to personal data transferred by means of other transfer mechanisms such as SCCs and BCRs. Indeed, in section 3.1.2 of the draft Commission Implementing Decision, the overview of effective legal protection in U.S. law is of general scope and not limited to data transfers made via the Shield. Also, in section 3.2 of its Communication (COM(2016) 117 final), the Commission explicitly indicates that such safeguards will apply to *all* personal data transferred to the U.S. for commercial purposes, not only to Shield transfers. This is a positive development because it becomes harder for European regulators or potential plaintiffs to argue that SCCs and BCRs would allegedly fail to meet the test laid down by the ECJ in the *Schrems* ruling with respect of U.S. government access to personal data.

3. Dispute Resolution

A potentially problematic issue is the multitude of avenues that individuals may use to lodge a complaint under the Shield. In practice, this may create a significant administrative burden for organizations, which will now have to be alert and ready to respond on many fronts.

First, individuals are encouraged to raise any concerns or complaints with the organization itself, which is obligated to respond within 45 days. Note that this is stricter than some European data protection laws (in France, for example, the timeframe is two months under current law). Under the Shield, individuals also have the option of working through their local DPA, which may contact the organization and/or the Department of Commerce to resolve the dispute.

The second avenue is an independent recourse mechanism. The Shield requires organizations to provide an independent recourse mechanism that will investigate and expeditiously resolve complaints and disputes at no cost to the individual. Organizations may select a private sector alternative dispute resolution ("ADR") provider or a panel of European DPAs. The private sector ADR provider must satisfy certain Shield requirements, such as responding promptly to inquiries and information requests from the Department of Commerce; reporting an organization's noncompliance to regulators, courts or the Department of Commerce; and issuing annual reports that provide aggregate statistics regarding their Shield ADR services. Organizations may also opt to use a panel of DPAs for their independent recourse mechanism. Note that this is mandatory if an organization uses the Shield for transfers of human resources data. In that case, the DPA panel will be competent to hear individual claims that have remained unresolved despite the organization's internal complaint handling efforts. Both parties will have an opportunity to provide comments and submit evidence before the DPA panel issues its "advice," which it will try to issue within 60 days. Once the advice is issued, organizations must comply within 25 days. Should an organization fail to comply, the DPA panel may either refer the matter to the Federal Trade Commission (FTC), or another body with statutory authority to enforce against unfair and deceptive trade practices, or inform the Department of Commerce that the organization should lose its Shield certification because it seriously breached its agreement to cooperate with the panel, and therefore that agreement is null and void.

For disputes or complaints involving human resources data that are not resolved internally by the organization (or through any applicable trade union grievance procedures) to the satisfaction of the employee, the organization is expected to direct the employee to the state or national DPA or labor authority in the jurisdiction where the employee works.

The Shield provides yet another dispute resolution mechanism, namely binding arbitration by the Privacy Shield Panel. This option is open to individuals who have raised their complaints with the organization, used the independent recourse mechanism and/or sought relief through their DPA but whose claimed violations still remain fully or partially unremedied. Note that arbitration is not available if a DPA has "authority to resolve the claimed violation directly with the organization." The Privacy Shield Panel is composed of one or three independent arbitrators admitted to practice law in the U.S., with expertise in U.S. and EU privacy law. The panel can only impose equitable relief, such as access or correction—it cannot award damages. Arbitrations should be concluded within 90 days. While the individual may not bring his or her claim for equitable relief in another forum after opting for arbitration, he or she may still file a claim for damages otherwise available in the courts. Furthermore, both parties may seek

judicial review of the arbitral decision under the U.S. Federal Arbitration Act.

In other words, after raising a complaint with the organization, petitioning the independent recourse mechanism, filing a complaint with the DPA and seeking equitable relief from the Privacy Shield Panel, the parties may still petition the courts (with the exception of individual complaints to the FTC or another U.S. statutory body).

In light of the above, a participating organization contemplating which data transfer compliance mechanism to implement may be discouraged by this wide array of avenues and potential fronts. For comparison, the SCCs (both Controller-to-Processor and Controller-to-Controller) provide for dispute resolution either by mediation or by the courts of the EU member state in which the data exporter is established. Also, for BCRs, the dispute resolution mechanisms seem less burdensome, as they provide for an internal complaint handling process, lodging complaints with competent DPAs and before the courts either at the data exporter's location or at the location of the EU headquarters of the organization.

4. Enforcement Authorities

In addition to adding several channels through which an organization may be confronted with individual complaints, other types of enforcement are expanded as well. An organization's compliance with the Shield may be directly or indirectly monitored by the Department of Commerce, the FTC, the Department of Transportation (or other body with statutory authority), European DPAs and private sector independent recourse mechanisms or other privacy selfregulatory bodies.

Under the Shield, the Department of Commerce will significantly expand its role in monitoring and supervising compliance. To accomplish this new mission, the Department of Commerce has doubled the size of the program staff and has committed to dedicating the resources necessary to ensure effective monitoring and administration of the program. Some of the Department of Commerce's new responsibilities include:

- Serving as a liaison between organizations and DPAs for Shield compliance issues;
- Verifying self-certification requirements by evaluating, among other things, the organization's privacy policy for the required elements and verifying the organization's registration with an ADR provider;
- Conducting periodic *ex officio* compliance reviews which will include sending questionnaires to participating organizations to identify issues that may warrant further follow up action. In particular, such reviews will take place when the Department of Commerce has received complaints about the organization's compliance, the organization does not respond satisfactorily to its inquiries and information requests or there is "credible" evidence that the organization does not comply with its commitments. Organizations will be required to provide a copy of the privacy provisions in their service provider contracts upon request. The Department will consult with the appropriate DPAs when necessary;
- Conducting *ex officio* investigations of those who withdraw from the program or fail to recertify to verify that such organizations are not making any false claims regarding their participation. In the event that it finds any false claims, it will first issue a warning, and then, if the matter is not resolved, refer the matter to the appropriate regulator for enforcement action; and
- Conducting searches for false claims by organizations that have never participated in the program and taking the aforementioned corrective action when such false claims are found.

The FTC will give priority consideration to Shield compliance issues raised by the Department of Commerce and European DPAs. In particular, it is designating an agency point of contact, creating its own standardized referral process to facilitate referrals from the DPAs and providing guidance to the DPAs on the type of information that would best assist the FTC in its inquiry into a referral.

Private sector independent recourse mechanisms will have a duty to actively report organizations' failures to comply with their rulings to the Department of Commerce. Upon receipt of such notification, the Department will remove the organization from the Shield List.

Both individual DPAs and the DPA panel will be able to refer complaints regarding Shield compliance to the Department of Commerce. Of course, the DPAs also have the authority to address organizations directly if they process HR data or have committed to cooperate with DPAs.

The above overview illustrates the complexity of the new agreement and the multiplication of authorities in charge of oversight, all of which is likely to result in greater regulatory scrutiny of and compliance costs for participating organizations. By way of contrast, when an organization relies on alternative transfer mechanisms such as the SCCs, the regulatory oversight is performed by EU regulators against the EU company (as data exporter). Therefore, before settling on a transfer

mechanism, organizations will want to consider the regulatory involvement and compliance costs associated with each option.

5. Reporting and Continuing Compliance Obligations

Finally, participating organizations will be subjected to additional compliance and reporting obligations, some of which will continue even after withdrawal from the Shield. As was required under the Safe Harbor, organizations must recertify their compliance on an annual basis. In addition, Shield organizations will now be required to maintain records regarding the implementation of their privacy program and provide them to regulators upon request.

Like the Safe Harbor, organizations that leave the Shield program for any reason must continue to protect the information received during their participation in the program in accordance with the Principles. However, the Shield adds a new reporting requirement for these organizations. For as long as they retain the information, they must affirm annually to the Department of Commerce that they are protecting the information in accordance with the Principles. Otherwise, the organization must return or delete the information or provide "adequate" protection for the information by another authorized means (*e.g.*, SCCs).

CONCLUSION

The text of the proposed EU-U.S. Shield signals the intention of the EU and U.S. governments to work together to address the gap in data transfer mechanisms left by the *Schrems* ruling. But it also underlines the complexity and depth of the differences in the way the two systems approach privacy. It remains to be seen whether and to what extent the Shield in its current form appropriately addresses the concerns of all interested parties: privacy concerns of citizens, legal requirements of the ECJ and legitimate practical considerations of companies wishing to comply on both side of the Atlantic.

There are indications already that the Commission may face some challenges to finalizing the deal in the coming weeks. On April 13, 2016, the WP29 issued its non-binding opinion on the Shield which identified a number of shortcomings and requested clarifications with respect to redress mechanisms, the Ombudsman and restrictions on mass surveillance, among others. The Commission will now consider the WP29's comments and decide whether to negotiate further changes before submitting its draft adequacy decision to the Article 31 Committee of EU Member States' representatives. The Article 31 Committee must issue an opinion before a final adequacy decision can be issued. After that, the adequacy decision will go through the committee procedure before it is formally adopted.

Companies should give careful consideration to the potential advantages and disadvantages of the Shield in comparison with other transfer tools such as SCCs and BCRs. The complexity of the new agreement and the increased cost of compliance underscore that the Shield goes far beyond a mere upgrade of Safe Harbor. Also, although the Shield may withstand judicial scrutiny this year, the ECJ warned that adequacy determinations are an ongoing process, hence the inclusion of an annual review process involving EU and U.S. authorities. What the consequences of this process will be for companies is unclear: if the result of annual reviews is to add new requirements on top of existing ones as issues arise, it may very well turn the Shield into a moving compliance target.

DIGITAL SINGLE MARKET STRATEGY UPDATE: EUROPE PROPOSES FURTHER HARMONIZATION OF CONSUMER PROTECTION LAWS

By Susan McLean and Kristina Ehle

The European Commission has published two draft directives on the supply of digital content and the online sale of goods that aim to help harmonize consumer law across Europe. In proposing these new laws, the European Union is making progress towards one of the main goals in its Digital Single Market Strategy (announced in May 2015), which is concerned with strengthening the European digital economy and increasing consumer confidence in online trading across EU Member States. According to the Commission, only 12% of EU retailers sell online to consumers in other EU countries, while more than three times as many sell online in their own country. The Commission has also announced a plan to carry out a fitness check of other existing European consumer protection laws.

This article outlines the potential implications of these latest developments, with a particular focus on the UK and Germany.

DIGITAL CONTENT AND ONLINE SALES OF GOODS

This is not the first time that the Commission has tried to align consumer laws across the EU: the Commission's last attempt at a Common European Sales Law faltered in 2015. But the Commission has now proposed two new directives dealing with contracts for the supply of digital content ("Draft Digital Content Directive") and sales of online goods ("Draft Online Goods Directive") (together, the "Proposed

Directives"). The Online Goods Directive will replace certain aspects of an Existing Sales of Consumer Goods and Associated Guarantees Directive ("Existing Goods Directive"), whereas the Digital Content Directive introduces a new set of rights for consumers when they buy digital content across the EU.

Part of the issue with previous EU legislative initiatives in this area is that "harmonized" has really meant "the same as long as a country doesn't want to do anything different." This time, the Proposed Directives have been drafted as so-called "maximum harmonization measures," which would preclude Member States from providing any greater or lesser protection for the matters falling within their scope. The Commission hopes that this consistent approach across Member States will encourage consumers to enter into transactions across EU borders, while also allowing suppliers to simplify their legal documentation by using a single set of terms and conditions for all customers within the EU.

The Proposed Directives will need to be adopted by the EU Parliament and Council before becoming law. Member States would then have two years to transpose the Proposed Directives into national law.

CONSUMER PROTECTION FITNESS CHECK

Following publication of the Proposed Directives, the Commission also published a roadmap setting out its plan to carry out a "fitness check" of six consumer protection directives (the Misleading and Comparative Directive, Unfair Commercial Practices Directive, Price Indication Directive, Unfair Contract Terms Directive, Sales and Guarantee Directive and Injunctions Directive ("CP Directives")), with the aim of assessing the effectiveness, efficiency, coherence and relevance of the CP Directives.

The Commission will look at the extent to which the fundamental objectives of the CP Directives have been achieved, whether further harmonisation is necessary, whether there is potential for complication of the current regulatory framework and whether there is scope of consolidation of EU consumer law. The Commission will also consider whether the Unfair Contract Terms Directive should be reinforced by a blacklist of terms that are always deemed to be unfair.

In addition, the Commission wishes to look at whether consumer rules should also apply in business-to- business (B2B) transactions, in particular, transactions with small and medium-sized enterprises (SMEs) and not-for-profit entities that don't qualify as consumers under the current rules. Lastly (with the rise of the sharing economy in mind), the Commission wants to review the issues arising in both consumer-to-consumer transactions and consumer-to-business relations.

The Proposed Directives will be taken into account when the fitness check is being performed, and are expected to have an impact on the Commission's findings in these areas.

The Commission will also consider as part of this review sector-specific consumer protection directives and EU legislation related to retail commerce, such as the E-Commerce Directive and the Services Directive, both of which contain consumer information requirements.

Evidence will be gathered during 2016, including via an online public consultation, and the Commission aims to publish its report on the results of the fitness check in the second quarter of 2017.

The Commission is also carrying out a separate review of the existing Consumer Rights Directive (CRD) which has been in force since June 2014, and the results of that review will also feed into the fitness check.

DRAFT DIGITAL CONTENT DIRECTIVE

Scope

The Draft Digital Content Directive would apply only in business-to-consumer sales and would not extend to SMEs. In addition, digital content providers in certain sectors, such as financial services, gambling or health care, are outside the scope of the directive. The rules would apply: (i) regardless of the method of sale (unlike the Draft Online Goods Directive) and (ii) to both digital content sold to the consumer (i.e., licensed on a perpetual basis) and digital content supplied under a temporary license. Currently, most EU Member States do not have national consumer protection legislation specifically concerning sales of digital content to consumers (the issue tends to be covered by sales of goods or services rules). The Commission believes that there is a risk of further legal fragmentation if no action is taken at the EU level.

The key provisions of the Draft Digital Content Directive include:

- **Supplier's liability for defects:** If the digital content is defective, the consumer can request that the defect be fixed. This can be done by the supplier providing an update of the content, or by asking the consumer to access/download a new copy of the digital content. There will be no time limit for the supplier's liability for such defects because, unlike goods, digital content is not subject to "wear and tear."

- **Reversal of burden of proof:** If the digital content is defective, it will be the supplier's responsibility to prove that the defect did not exist at the time of supply. The Commission believes that this is important because the technical nature of digital content means that it can be difficult for consumers to prove the cause of a problem. Software companies have criticized this approach on the basis that they believe that it will be

The Commission will look at the extent to which the fundamental objectives of the CP Directives have been achieved, whether further harmonization is necessary, whether there is potential for complication of the current regulatory framework and whether there is scope of consolidation of EU consumer law.

almost impossible for them to prove that their digital products were not defective. The proper function of software depends on the hardware, operating system and other software used on the consumer's systems; any interfaces to those systems or incorrect use of the software may be responsible for an issue. Analyzing and identifying the issue would mean that the provider would have to access the consumer's system, and providers argue that this would cause unreasonable effort and costs for the provider.

- **Right to end a contract:** Consumers will have the right to terminate long-term contracts and contracts to which the supplier makes major changes.

- **Contract established in exchange for data:** If the consumer has obtained digital content or a service in exchange for personal data, the new rules clarify that the supplier should stop using the data when the contract terminates.

IMPLICATIONS FOR THE UK

Since October 1, 2015, UK consumers have enjoyed new rights and remedies with respect to digital content under the Consumer Rights Act (CRA). The Draft Digital Content Directive would reduce UK consumer protection in some areas and enhance it in others. Accordingly, various concerns have been raised by the UK's Department for Business, Innovation & Skills (BIS), the UK's competition regulator (CMA) and the UK's Chartered Trading Standards Institute (CTSI).

- **Scope:** The Draft Digital Content Directive applies to a broader range of digital content than the CRA. In particular, the CRA applies only where digital content has been paid for. The Directive extends remedies to "free" content in that the Directive covers content that is provided for non-monetary consideration, e.g., in exchange for the consumer actively providing personal data. BIS suggests that the concept of "actively providing" data is not clear. Does this simply require a positive action by the consumer? Is simply agreeing to make data available sufficient to pass this test? The CMA believes that consumers would need to do more than, say, "click" a button. Whereas BIS states that extending rights to cover free services may not be proportionate, the CMA broadly welcomes the proposed approach but suggests how this works in practice will need careful consideration. The Draft Digital Content Directive also extends to certain types of digital services not currently covered in the CRA (e.g., cloud storage services and social networking). However, BIS believes that the Directive could be clearer as to which services are covered and which are not, to avoid overlap/conflict with other EU legislation.

- **Data protection:** BIS states that although the Draft Digital Content Directive has been drafted without prejudice to applicable data protection law, "any confusion with or unjustified extension of the already comprehensive EU rules in this area including the GDPR should be avoided."

- **Installation of digital content:** The Draft Digital Content Directive introduces new provisions regarding installation that are not included in the CRA.

- **Modification of digital content:** Under the Draft Digital Content Directive, more restrictions are imposed on modifications by suppliers, and consumers have a new right to terminate the contract if the trader makes a modification that adversely affects access to or use of the digital content. Although it agrees with the general thrust, the CMA has concerns that a trader's right to update content shouldn't be used to dilute consumer control.

- **Standards and remedies:** BIS believes that the approach to standards in the Draft Digital Content Directive (i.e., fit for a specific purpose, as described and of satisfactory quality) will have the same effect as the applicable provisions in the CRA. However, BIS points out that they are not in line with the regime in the Online Goods Directive, which isn't helpful. The CMA agrees that alignment would help avoid market distortions and uncertainty.

- **Reversal of the burden of proof:** Currently in the UK there is an assumption that digital content must comply with its contract for six months after purchase. Under the Digital Content Directive, this reversal of the burden of proof has the potential to continue for a considerably longer period.

- **Termination:** The Draft Digital Content Directive introduces a new right to terminate after one year any contract of indefinite length or that extends beyond one year. In addition, with respect to the new rules on the return of consumer data, BIS believes that these rules appear very broad (beyond what is required under data protection law) and potentially onerous. BIS suggests that it could be difficult for the trader to retrieve this data which "would appear to be of little practical use to the consumer."

IMPLICATIONS FOR GERMANY

In Germany, no statutory consumer law specific to digital content currently exists. Instead, German courts apply general laws on the sale or rental of items (including consumer-specific rules) where digital content is provided in exchange for payment. Where the digital content is provided in exchange for non-monetary considerations (e.g., user-generated content or user data), the statutory rules on barter contracts apply. The Draft Digital Content Directive would constitute the first comprehensive legal framework for the supply of digital content in Germany.

- **Standards and remedies:** Under the Draft Digital Content Directive, digital content needs to be in conformity with the contract or, where the contract is silent, to at least be fit for ordinary use. These rules explicitly determine conformity of digital content by mirroring the corresponding rules of the Existing Goods Directive. Therefore, only a few changes to German law will be required, as many of the existing rules are already applied to digital content in Germany.

- **Reversal of the burden of proof:** The reversal of the burden of proof provisions in the Existing Goods Directive, which state that consumer goods are considered to have been defective at the time of delivery if a defect is found within six months, currently only apply to physical goods. In particular, with regard to digital content licensed for a limited term only (which is considered a rental contract and not a sales transaction), the burden of proof is currently with the licensee. The permanent reversal of the burden of proof for digital content under the Draft Digital Content Directive would be an entirely new concept under German law.

- **Right to damages:** The Draft Digital Content Directive stipulates that consumers are entitled to damages caused by the defective content. As the German Civil Code generally provides for comprehensive rules on compensation of economic damages, we do not expect that substantive changes will be required.

- **Termination:** The termination right for long-term contracts after one year (as contemplated by the Draft Digital Content Directive) would enhance existing German consumer protection law. Under existing law, contract terms of up to two years are enforceable in standard agreements with consumers.

- **Reimbursement:** Under the Draft Digital Content Directive, following termination, the seller must reimburse the purchase price or, where the content was provided in exchange for non-monetary consideration, refrain from using what the seller received from the consumer (e.g., the user-generated content or data). The latter provision extends consumers' rights under German law.

DRAFT ONLINE GOODS DIRECTIVE

Like the Draft Digital Content Directive, the Draft Online Goods Directive would only apply in business-to-consumer sales. Only goods sold online or otherwise at a distance fall within its scope. As such, any face-to-face sales are not covered. Contracts for the supply of services would not be subject to the Directive. Where a contract is for the supply of both goods and services, the rules would apply only to those elements of the contract that relate to goods.

The key provisions of the Draft Online Goods Directive include:

- **Reversal of the burden of proof for two years:** Under existing law, a consumer asking for a remedy for a defective product does not have to prove that the defect existed at the time of delivery; it is up to the seller to prove that the defect did not exist. Currently, the time period during which the seller has this burden of proof varies by Member State; under the new law, this period will be extended up to two years throughout the EU.

- **No notification duty:** Consumers won't lose their rights if they don't inform the seller of a defect within a certain period of time (as is currently the case in some Member States).

- **Minor defects:** If the seller is unable or fails to repair or replace a defective product, consumers will have the right to terminate the contract and be reimbursed. This is also true in cases of minor defects.

- **Secondhand goods:** For secondhand goods purchased online, consumers will now have the possibility to exercise their rights within a two-year period, as is the case with new goods,

instead of the one-year period that currently applies in some Member States.

IMPLICATIONS FOR THE UK

The Draft Online Goods Directive retains many of the same key rights and remedies set out in the Existing Goods Directive and recently implemented in the UK under the CRA. However, there are some differences between the statutory remedies proposed in the Draft Online Goods Directive and the CRA and it's likely that a number of key rights under the CRA would likely need to be repealed for online and other distance sales, which has led to concerns being raised by BIS, CMA and CTSI, in particular:

- **Short-term right to reject:** Under the CRA, consumers have a right to reject and obtain a full refund within 30 days. This would need to be repealed in relation to goods purchased online. However, consumers' rights under the CRD would not be affected so consumers would still be entitled to a 14-day right of withdrawal for goods bought online or at a distance. However, unlike the short-term right to reject, the consumer has to bear the cost of returning the goods under the right to withdraw and the trader may make a deduction for use from the refund, depending on the circumstances. CTSI sees this proposed change as a retrograde step and doesn't consider the CRD provisions sufficient to ameliorate the problems caused by the removal of the right to reject. The CMA is also unhappy with the change, believing it would reduce certainty, to the disadvantage of both consumer and trader.

- **Loss of one repair or replacement limit:** Under the CRA, consumers can pursue a price reduction or refund after the goods have undergone one repair or replacement. This would need to be repealed. The UK would be required to reinstate the law that existed before the CRA which, according to CTSI, lacked clarity and led to significant consumer frustration, i.e., consumers can ask for a price reduction or refund if a repair/replacement cannot be provided within a *reasonable time and without significant inconvenience*. The CMA also disagrees with the removal of this key protection and recommends the draft Online Goods Directive be amended in line with the CRA.

- **Liability period:** Currently, the liability and limitation periods for remedies are six years in England, Wales and Northern Ireland and five years in Scotland. The Draft Online Goods Directive would reduce the liability period (i.e., the period in which a fault has to appear before a consumer can make a claim) to two years. Again, CTSI and CMA don't support this change, believing it a significant reduction in consumer rights.

- **Deduction for use:** The approach to deduction for use under the CRA is different and would need to be updated. Under the CRA, if a repair or replacement is impossible or has failed or has not been carried out in a reasonable time or without significant inconvenience to the consumer, then the consumer may reject the goods and obtain a refund. If the final right to reject is exercised within six months of delivery of the goods, then the trader must generally give the consumer a full refund. After the first six months, the trader may apply a deduction to the refund to account for the consumer's use.

On the other hand, the Draft Online Goods Directive will enhance consumer protection under the CRA by extending the reversal of the burden of proof from six months to two years. During this extended period, it will be the responsibility of the supplier to prove that the goods were satisfactory at the time of sale. On this point, CTSI is not supportive as it says it is not sure this enhancement strikes the right balance and it may be unfair to businesses. The CMA supports the proposal in principle, but the proposal doesn't offset its concerns regarding the reductions in consumer protection introduced by the draft Online Goods Directive.

Other concerns have been raised in the UK. For example, suppliers operating in the UK would be subject to different rules depending on the method they use to supply goods: offline selling would fall within the scope of the CRA, whereas online or distance selling would engage the provisions of the Proposed Directives. Suppliers using both methods would be required to comply with both sets of rules, and there are concerns from both CTSI and CMA that this could lead to confusion for consumers, and challenges for suppliers juggling two different sets of rights. CMA also points out that the different rules could lead to market distortion, with consumers more inclined to buy offline, thus reducing online growth.

IMPLICATIONS FOR GERMANY

The Existing Goods Directive, which is amended by the Draft Online Goods Directive, is currently transposed into the German Civil Code.

It is worth noting that in Germany, with the exception of the provisions on the trader's redress, the reversal of the burden of proof, some features of the consumer guarantee and the mandatory nature of the rules, most of the rules of the Existing Goods Directive have been extended to non-consumer sales contracts. It remains to be seen whether a similar extension will be made with regard to the changes in the Draft Online Goods Directive, which would impact B2B e-commerce transactions.

- **Reversal of the burden of proof:** As set forth in the Existing Goods Directive, under existing German law, if there is a defect within the first six months following delivery of goods, the burden of proof that the delivered goods were not defective at the time of delivery lies with the supplier. The Draft Online Goods Directive would extend this reversal of the burden of proof to two years. It remains to be seen how this reversal of the burden of proof would be treated by the German courts that have tended to minimize the impact of the existing reversal.

- **No notification duty:** There is no notification duty with regard to defects for consumers under current German law, so its abolition in the Draft Online Goods Directive would not impact German law.

- **Minor defects:** German law currently only provides for a proportionate reduction of the purchase price in case of minor defects but not for a termination right. A right to terminate would be an extension of consumer rights under German law.

- **Liability period:** Currently, sellers in Germany are already liable for defective goods sold online for two years after the sale, which is the corresponding statute of limitations. Consequently, there will be no change under the Draft Online Goods Directive.

- **Reimbursement for returns:** Under existing German law, the seller may refuse to reimburse the buyer until the goods have been returned. The Draft Online Goods Directive requires the seller to reimburse the consumer within 14 days from receipt of the termination notice.

- **Compensation for decrease in value:** Consumer sales law in Germany currently prohibits deduction for use and compensation of value when a consumer terminates the sales contract. The Draft Online Goods requires the consumer to pay for a decrease in the value of the goods insofar as the decrease exceeds depreciation through regular use.

CONCLUSION

Although the Proposed Directives still have a long way to go before they become law, they demonstrate that there is a keen desire for harmonization at the EU level.

Being able to have one set of terms and conditions for all customers in Europe would certainly appeal to many businesses that already offer, or would like to offer, consistent terms for their cross-border sales to consumers and are currently navigating a patchwork of consumer laws.

A possible alternative would have been to apply the consumer law of the home country of the respective provider also to transactions with consumers seated in another Member State. The E-Commerce Directive (2000/31/EC) is an example of this "country of origin principle." This alternative approach not only would benefit the businesses actually involved in cross-border e-commerce, but would also prevent additional costs and efforts for many SMEs that do not aim to do cross-border business but, nevertheless, would have to implement the new fully harmonized consumer rules proposed by the Commission.