



Hogan
Lovells

GMCQ

Global Media Technology and
Communications Quarterly

Autumn/Winter 18

Editorial

New laws and proposals are being introduced all around the world focusing on the protection of privacy and data in the digital economy. Hot on the heels of the European Union's General Data Protection Regulation (GDPR), which came into force in May this year, a groundbreaking new data privacy law has been passed in California, with extensive compliance requirements and significant enforcement and class action liability provisions. Hogan Lovells Washington D.C. partners Mark W. Brennan and Tim Tobin lead this issue of the Global Media Technology and Communications Quarterly with their explanation of the impact of the new California privacy law on TMT sector companies doing business in California.

Staying on the theme of data privacy and the digital economy, Eduardo Ustaran, co-head of the Hogan Lovells privacy practice, follows Mark Brennan and Tim Tobin's article with his comments on the increasingly popular use of personal data to tailor and personalise the consumer experience of the Internet and what digital companies can do to ensure they stay within the rules of the GDPR and e-privacy law.

We also have two substantial extracts from our global thought leadership. On p.18, we have an extract from US academic Robert W. Crandall's

white paper on the effects of technological change on US regulatory policies in the communications sector, which has been prepared with T-Mobile and Hogan Lovells. And on p.33 we have a sneak preview of an extract of a chapter written by Hogan Lovells partners Winston J. Maxwell, Jason D. Lohr and Peter Watts, on regulating AI, for a forthcoming publication, *Algorithmic Regulation*, by Oxford University Press.

With tens of billions of connected devices predicted to be in use by 2020, there is a growing emphasis on the importance of IoT-related product safety and liability. On p.12, Hogan Lovells partner, Valerie Kenyon, from our London office, talks about how the product safety and liability regulatory landscape in Europe and the UK for connected devices is changing and evolving with advances in technology.

Finally, on p.26, our China TMT partners explain China's new and first e-commerce law, which comes into force on 1 January 2019, regulating the rapidly growing e-commerce sector in China and Hong Kong. The real aim of the new law, the authors say, is to try and bring some order to what has become a successful but unruly sector of the Chinese economy.



Winston Maxwell
Partner
Paris



Trey Hanbury
Partner
Washington, D.C.



Penelope Thornton
Senior Associate
London

Contents

| | |
|----|---|
| 04 | The new California consumer privacy law: what you need to know |
| 10 | Personalisation is the new black |
| 12 | How IOT could redefine EU product safety and liability in the EU Q&A with Valerie Kenyon |
| 18 | The effects of rapid technological change on us regulatory policies in the communications sector |
| 26 | A game changer? China enacts first e-commerce law |
| 33 | Using contracts to manage AI risk |
| 37 | References |



The new California consumer privacy law: what you need to know

A new U.S. state privacy law has been passed in California with extensive compliance requirements and significant enforcement and class action liability provisions. The California Consumer Privacy Act of 2018 ("CCPA" or the "Act") applies to most entities that do business in California (potentially even if they have no offices there and merely invest in businesses operating in California) and that collect the personal data of California residents. If you have customers that are California residents, handle California consumers' information, or have employees in California, it may apply. The CCPA also may influence the direction of other U.S. federal and/or state privacy legislation. Even though it is not effective until January 1, 2020, because some of the CCPA provisions reach back twelve months, companies should start their compliance planning now, including for data mapping and business impact reviews. In this article, we provide additional details on the Act and its potential impact for TMT sector companies, along with a high-level comparison to the GDPR.

A groundbreaking new privacy law

On June 28, 2018, California's governor signed Assembly Bill 375, a groundbreaking new data privacy law that some are comparing to the European Union's General Data Protection Regulation (GDPR). The CCPA will significantly impact how technology, media, and telecoms companies that operate in California may collect, sell, and disclose consumers' personal information. In fact, even though the law will have an impact across sectors, it is notable that the perceived practices of large TMT sector companies is what drove enactment of the CCPA, following a compromise that would have resulted in an even more onerous ballot initiative appearing before California voters in November 2018.

Bottom line

The law will require covered businesses – including many technology companies operating in California – to: make certain public disclosures about personal information collection and use; grant consumers (defined as natural persons who are residents of California, which as explained below may result in broad applicability) access to details about the collection and use of their personal information, including the sources of information; delete consumers' personal information upon a consumer's request unless

“

“The perceived practices of large TMT sector companies is what drove enactment of the CCPA.”

”

certain exceptions apply; provide consumers a right to opt out of the sale of their personal information (minors under the age of 16 must affirmatively assent to such a sale); and comply with other requirements.

The Act also includes anti-discrimination provisions that limit businesses' ability to deny services, charge different prices, or offer different qualities of service to consumers who exercise their rights.

Doing business

The Act applies to all companies that do business in California. Although we expect further guidance (including potentially from the Attorney General) on this point, California courts have historically interpreted the concept of "doing business" broadly. In some instances, companies may "do business" in California even if they do not have physical offices in the state. And companies may even be "doing business" just by investing in companies that operate in California.

Enforcement

The California Attorney General will have primary enforcement responsibility and authority to impose civil penalties for up to US\$7,500 per intentional violation. However, the law also allows consumers, under some circumstances, to bring private actions for certain data incidents that result from businesses' failure to maintain reasonable security procedures.

The law requires the Attorney General to complete a rulemaking by July 1, 2020 (six months after the Act's effective date, assuming that recent amendments passed by the California legislature are signed into law by the governor) to implement the CCPA and provide guidance to affected stakeholders.

Additional details and potential impact

- The CCPA broadly defines "**personal information**" to include almost any information (including inferences) that could be linked to an individual, household, family, or device. Notably for TMT companies, this includes a broad array of online data such as cookie numbers, IP addresses, MAC addresses and device IDs, online browsing or search activities, and third party data, including offline data, merged with any of this information. Companies that have traditionally considered information to be personal information only if it reasonably identifies a specific person will need to update their disclosures and compliance practices, and consider strategies for mapping and locating such information to comply with the various individual rights.
- The definition of "**consumer**" is worded such that employees appear to be covered and therefore they are entitled to the same rights as other consumers, subject to the Act's exceptions as applicable.

“

“The CCPA will significantly impact how TMT companies that operate in California may collect, sell, and disclose consumers' personal information.”

”

“

“Companies will need to assess and justify their determinations, which may involve substantial compliance costs.”

”

- There are a number of generally applicable **disclosure requirements**, an entity must address in its privacy policy or other consumer disclosures, including a description of consumer rights under the Act, the categories of personal information collected, and the purposes for which an entity uses such information.
- There are also a number of individualized **disclosure requirements** for consumer requests about the categories of personal information that a business collects, including its sources, and the categories of personal information sold or disclosed to third parties (generally reaching back twelve months).
- There is a **consumer right to access** the specific pieces of personal information that a business collects about the consumer, which has the potential to result in companies disclosing:
 - proprietary information regarding the types of data collected, the specific data held, and the inferences drawn from the data;
 - information associated with shared devices to abusive spouses or others; and
 - information in a portable format, allowing consumers to migrate to other businesses.
- The Act contains a **consumer right to delete personal information**. Although the CCPA includes a range of exceptions justifying retention, companies will need to assess and justify their determinations, which may involve substantial compliance costs.
- There is also a broad consumer right to opt out of the sale of personal information.
 - “Sale” is broadly defined to include the sharing of personal information with a third party for monetary or other valuable consideration.
 - Consumers can authorize third parties to opt out on their behalf. Consumer advocacy groups or other entities may develop broad opt-out tools to facilitate mass opt-outs. And an opt-out option has to be readily available through an opt-out logo or button.
 - Unless businesses share personal information for no consideration of any kind, consumers themselves intentionally share the personal information with specified third parties, or the recipients of personal information operate as pure service providers without any independent use including for internal product development, the opt-out right threatens to disrupt sharing arrangements.

- There are exceptions for various types of personal information, such as where such information is subject to the Gramm Leach Bliley Act, the California Confidentiality of Medical Information Act, the Health Insurance Portability and Accountability Act, the Driver's Privacy Protection Act, and some others regimes, but these exceptions will have limited applicability to most TMT companies.
- The **anti-discrimination provisions** may ultimately limit incentives for data monetization.
 - The Act generally prohibits discriminating against consumers for opting out of the sale of personal information or exercising data access or deletion rights.
 - Discrimination includes charging different prices or offering different service levels.
 - The Act permits incentives if the value of the incentives is reasonable in relation to the value provided to the consumer by the consumer's data. The Act does not clarify how to measure the value of personal information to consumers, so any attempts to rely on this provision must be carefully thought through.
- The Act requires **opt-in consent** to authorize the sale of personal information associated with **minors under age 16**.
- **Affiliate companies** that are under common control and share branding appear to be treated as a single business. As a result, data deletion, data access, and opt-out requests will need to be communicated and effected within certain affiliate groups that may lack interoperable systems.

Example actions that could trigger CCPA requirements for TMT companies due to a "collection" of "personal information" about California "consumers":

Receiving business card or contact information

Marketing and ad targeting

Research and data analytics

Handling human resources and employee data

Conducting investment diligence

Licensing/IP activities



Comparison to the GDPR

The CCPA is similar to the GDPR in some respects. For example, both have broad definitions of personal information and impose certain notice requirements. They also both allow data subjects to seek access to their data and delete their data under certain circumstances, and to make certain choices regarding the sale of their data. While the GDPR does not contain an explicit opt-out of sales provision, its other provisions operate to effectively provide that right in many circumstances.

One area where the Act goes beyond the GDPR is the anti-discrimination provision, which has no parallel in the GDPR. It also requires a “Do Not Sell My Personal Information” link on businesses’ homepages, whereas the GDPR does not.

On the other hand, unlike the GDPR, the CCPA does not require that all processing of personal data have a legal basis in the first instance or impose strict requirements for valid consent, strict requirements for the processing of sensitive personal data, requirements for contracts between data controllers and data processors, or requirements for transfers of personal data outside of the EU.

The GDPR’s right to erasure only applies in certain enumerated circumstances, but contains fewer exceptions than the CCPA deletion right. The CCPA deletion right generally applies to all personal data held by the business, but it is subject to several exceptions. The GDPR’s exceptions are more amorphous, however (e.g., where personal data is processed on the basis of legitimate interests, or where there is a “compelling” interest that outweighs the rights and freedoms of the individual).

With respect to enforcement, the GDPR allows private individuals to bring an action to enforce the regulation by seeking damages. The private right generally extends to all individual rights under the GDPR, and therefore goes beyond the more limited private right of action in the Act, although recovery based on actual damages is limiting. The GDPR is also enforced by data protection authorities throughout the EU member states. Violations of the GDPR can lead to penalties as high as 4% of gross global revenue. Depending on how violations are aggregated and the extent of a business's violations, the penalties under the Act could potentially exceed the GDPR's maximum 4% of revenue.

Summary

Businesses operating in California will need to keep a close watch on CCPA developments over the next year and a half, including on the anticipated Attorney General rulemaking expected to commence in 2019. In addition, because some of the CCPA provisions, such as information about sales or disclosures reach back twelve months, companies should start their compliance planning now, including for data mapping and business impact reviews (e.g., requests received on 1 January 2020 may have to be honored back to the beginning of 2019). We have also seen efforts to push for additional federal and state privacy legislation since the passage of the CCPA, and companies will want to keep a close watch on those developments.



Mark W. Brennan

Partner, Washington Office

T + 1 (202) 637 6409

Email: mark.brennan@hoganlovells.com



Tim Tobin

Partner, Washington Office

Tel: + 1 (202) 637 6833

Email: tim.tobin@hoganlovells.com

Personalisation is the new black

Internet innovation is in a state of flux. The GDPR is now in place and there is a strong feeling that some serious regulatory action for misuses of digital data is forthcoming. New laws and proposals around the world – from California and Brazil to India and China – are focusing on the protection of privacy and data in the digital economy, while the slow-burning legislative process to revamp the current e-privacy framework in Europe adds to the suspense.

Against this background, the commercial urge to tailor our experience of the Internet to our tastes, views of the world and personalities has never been greater. So it is probably not a coincidence that one of the most important strategic questions for digital businesses right now is how to justify personalisation in a world of continually evolving laws and increasingly complex rules.

The GDPR in particular, with its intricacies around the lawful grounds for processing, is a perfect testing ground for establishing the legitimacy of personalisation when accessing Internet-based content and services. In other words, under the GDPR, what is the soundest legal basis to use our personal data in order to provide us with tailored websites and apps? An obvious answer may, of course, be consent. But the legitimacy of consent as a realistic ground for data processing in a world where we have lost much control over the uses of that data is constantly being questioned.

Are we, humble Internet users, truly in a position to make an informed decision about data crunching practices that fly many, many miles over our heads? In short, do we have a genuine choice? Will we ever?

Given the pre-eminence and ever-growing importance of personalisation as a way of providing content, it is crucial to find a more sophisticated approach to this analysis to ensure that the legal basis for this practice is as solid as its commercial justification. An increasingly popular fall-back position when consent is challenged as a lawful ground is

“

“One of the most important strategic questions for digital businesses right now is how to justify personalisation in a world of continually evolving laws.”

”



'legitimate interests'. Seen as a panacea for justifying data uses by many but misunderstood by most, the legitimate interests ground is certainly available for pretty much every commercial use of personal data. But it comes with strong conditions which, in the context of digital personalisation involve careful thinking about potential privacy intrusions, actively embracing data minimisation and integrity, and above all challenge-proof transparency and control. In a nutshell, 'legitimate interests' can go a long way to legitimise data uses but it is crucial not to see it as a 'get out of jail free' card and to appreciate the considerable privacy-enhancing efforts that need to be made when relying on it.

The truly difficult question around the use of personal data for Internet personalisation is to what extent it can be argued that it is a 'contractual necessity'. Could it be said that for many digital businesses the ability to personalise what their customers see when they walk through their virtual door is an intrinsic part of the service they provide? Isn't it fair to say that without personal recommendations for books, music, films or running shoes, our online experience of some of the sites and services we use would be... well, useless? A narrow interpretation of what is necessary to enter into a contract may well rule out anything that doesn't involve purely transactional data, but is that the correct view of the world – that is, the digital world – in the 21st century? Everything is always debatable in data protection law but this is an area where a narrow interpretation of the law may be out of sync with our own expectations of the Internet.

Yet the law affecting this area is not restricted to the GDPR and in Europe alone, collecting and using data in this context also needs to be filtered through the layer of e-privacy law. Therefore, this issue is also affected by the rule requiring notice and consent to store information in devices and accessing it. Yes, the cookie consent rule! Are cookies aimed at helping personalisation strictly necessary to shop online? This is also debatable and, in fact, a very pressing legislative dilemma which proves how difficult it is to get the balance right.

Ultimately, this is all a matter of balance. It is about achieving the best of all possible worlds: control over our data and our digital lives on the one hand, and access to affordable and relevant products and services on the other. Those who get this right will be the most successful innovators of all.

This article was first published in Data protection Leader in September 2018.



Eduardo Ustaran

Partner, London Office

+ 44 (20) 7296 5249

Email: eduardo.ustaran@hoganlovells.com

How IOT could redefine EU product safety and liability in the EU

Q&A with Valerie Kenyon

How big is the Internet of Things (IoT)? It's likely that there will be tens of billions of connected devices in use by 2020. As this massive network of "things" keeps expanding, so do the number of questions about IoT-related product safety and liability issues.

When we're thinking about the standard of safety for IoT products, we need to look to the General Product Safety Directive (GPSD) and to other relevant product safety laws at both an EU and member state level.

In the event that a defective IoT product causes damage, the Product Liability Directive (PLD) is the key legislation that addresses product liability concerns. But advances in technology are outpacing the decades-old PLD. An evaluation now under way, however, should soon clarify some of the ambiguity arising from the evolving technology landscape, including new and more relevant definitions for defects, products, and producers.

In this interview, Valerie Kenyon, a partner focusing on product liability and safety in the Hogan Lovells London office, discusses the changes in and challenges to the EU's regulatory regime as the IoT continues to shape perceptions about product safety and liability.

Q: Why are we so interested in IoT safety and liability?

A: IoT devices have become part of our everyday lives. They're in the hands and the homes of every conceivable demographic — not just adults or the tech savvy, but also children, the elderly, and vulnerable users. So it's important that there are modern and clear rules around the safety and compliance of these devices, and that businesses in the IoT space are aware of these rules and the risks and liabilities they may face.

In the EU product regulatory landscape, IoT products fall within the scope of the GPSD. Let's spend some time looking at the way the GPSD applies to connected devices.

Q: How does the GPSD define a “safe” product?

A: According to the GPSD, a safe product “does not present any risk, or only the minimum risks compatible with the product’s use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons.”

The definition of a safe IoT product depends, in fact, on a host of factors, including the product’s characteristics, composition, packaging, instructions, interaction with other products, safety warnings, and the categories of consumers likely to use it. So we can already see that IoT products are going to throw up some questions that we wouldn’t necessarily need to think about in relation to conventional, nonconnected, electronic devices.

One question is, as a manufacturer, how do you warn about safety risks? If the consumer must have a mobile phone or an app in order to use the device, is it okay to give them safety information only on the phone or the app? In fact, is it preferable?

What about software? How do you feel about the situation in terms of safety, where a consumer has decided not to update their device with the latest safety-related patch? If something goes wrong, is the product to blame, or the consumer? And what about data-related risks, e.g. questions around hacking and cybersecurity?

These are just a few of the questions we’re helping businesses with in the IoT product space. And some of these are really challenging issues, keeping experienced manufacturers, importers, and distributors very busy.

Q: How is the EU legislator addressing these IoT-related issues?

A: The EU legislator is trying to keep up with these questions and develop policy in this area. In fact, we worked with the European Commission and the Alliance for Internet of Things Innovation (AIOTI) on recent policy documentation and raised these kinds of questions in relation to product safety and liability. In the United States, the Consumer Products Safety Commission (CSPC) had a public hearing on 16 May 2018 to receive information from all interested parties about potential safety issues and hazards with IoT products. It's important to keep an eye on the developing global landscape.

“

“For emerging technologies, standards often cannot keep pace with the speed of product change and innovation.”

”

Q: Where do IoT device manufacturers get the information they need to stay compliant?

A: Our team is constantly working within the realm of the GPSD and product safety laws. There's a range of EU product laws that may apply to your IoT product, depending on its features and characteristics. Typically, it's the responsibility of the manufacturer to ensure their devices are compliant, appropriately marked and labeled, and accompanied by the right documentation. Harmonized standards are very often used as a means of achieving compliance with EU product safety laws. But for emerging technologies, standards often cannot keep pace with the speed of product change and innovation.

Importers and distributors of IoT products have responsibilities, too. And it's important to know and understand your position in the supply chain to know how each relevant product safety law is going to affect you.

Again, for IoT products, this kicks up a number of compliance questions, and they're not necessarily all related to safety. For example, if your connected product doesn't fall squarely within any of the existing harmonized (or nonharmonized) standards, what's the best way to help establish that your product is compliant? To what standard should you test?

Q: Which connected devices may need to comply with additional regulations?

A: Depending on the device, additional regulations may apply. For example, aviation rules will be relevant in the context of drones, and automotive rules would apply to connected cars. New technology can really show up gaps and challenges in the applicable regulatory regime.

Q: You've said that it's important to think about IoT products and liability, even at this early stage.

Why is that?

A: First, it's really important to reassure people. We want consumers to buy these products, know how brilliant they are, and how they can shape the world. And consumers want to know that it's safe to do so. Unfortunately, there's been some scaremongering in the press about IoT products, which is not especially helpful to this emerging technology.

We're also seeing stories about real-life dangers arising from connected products. Autonomous cars, at the moment, are one example. We need modern and appropriate safety and liability regimes so that consumers and regulators can be more comfortable, and so that businesses have more certainty.

Q: What is the role of the PLD in the EU?

A: When we talk about liability for IoT products in the EU, we're talking primarily about the PLD plus local laws, such as negligence and contract liability.

The PLD sets out key provisions on liability, burden of proof, and what makes a product "defective." Here are three of the main features of the PLD: the first is that the producer shall be liable for the damage caused by a defect in a product. The second is that the injured person has to prove the damage, the defect, and the causal relationship between defect and damage. The third key point is that a product is defective when it does not provide the safety that a person is entitled to expect, taking all circumstances into account.

Q: Can you provide a high-level overview of the PLD's application to IoT products?

A: There's a real question mark about how each of the aspects we just mentioned apply to complex, connected IoT products. For example, does the meaning of a product extend to software and apps and the way that products communicate? Should a defect in an app for a product that causes harm come within the scope of the PLD? And who should be held responsible? For instance, if a network outage causes an accident, should the network provider be held responsible? And if a cyber attack causes an accident, is the manufacturer at fault for failing to make their product sufficiently safe against future cyber attacks? Or did the hacker's acts intervene?

These are interesting questions. What about, in the context of the consumer, if you fail to install an important safety-related software patch? At some point, do we think that the requirement and responsibility for safety should move toward the consumer if they fail to make fundamental software updates?

Q: Where are we heading next? In the context of connected products, is cybersecurity the new product safety, and is data litigation the new product liability?**What is the future of the PLD, in the context of the IoT?**

A: The PLD came into force in 1985 – some 30 years ago. The world was a very different place. Products were very different. You won't be surprised to hear that the European Commission has been evaluating the PLD in light of new technologies.

A number of consultations have already happened and there are more of them in the future.

“

“There's a real question mark about how each of the aspects apply to complex, connected IoT products of the PLD.”

”

The most recent consultation addressed a number of issues relating to IoT products and technology – for example, whether apps and nonembedded software should be within the scope of the liability regime. Also, whether the unintended, autonomous behavior of an advanced robot could be considered to be a defect. Another example is how strict liability for damage caused by IoT products should be allocated among the different parties involved. This issue is particularly complex in the case of a connected object or sensor that relies on information from another object or sensor, which isn't necessarily in the control of a single producer.

The Commission has recently released an updated report on the application of the PLD as well as a comprehensive evaluation of its implementation in practice. These make clear that, although the Commission still considers that the PLD continues to be an adequate tool, rapidly evolving technologies may mean that well-established principles of the Directive need to be reconsidered.

It was acknowledged that concepts like "product," "producer," "defect," and "damage" might need to be reevaluated to take into account the fact that products can be produced in complex supply chains with numerous contributors and incorporate software and other service components developed by other manufacturers.

The Commission also considered the debate on the allocation of extent of the burden of proof but came to the conclusion that the requirement that an injured person should have to prove the link between the damage and the defect should continue.

Another key area for the Commission was the overlap between product liability and cybersecurity, noting that "consumers and businesses need to be aware of the security levels they can expect, and they need to know who to turn to if a failing in cybersecurity leads to material damage."

“

“Although the Commission still considers that the PLD continues to be an adequate tool, rapidly evolving technologies may mean that well-established principles of the Directive need to be reconsidered.”

”

Q: So where are we now?

A: In addition to the consultations on the future of the PLD, the European Commission set up two new expert groups – one on liability, the other in relation to new technology. Both are considering things like IoT and the product liability regime with the aim of reviewing the applicability of the PLD and developing principles to guide the adaptation of existing EU laws to deal with the potential challenges raised by new technology. At the same time it is considering the wider implications of AI technology, with the creation of an AI technology expert group to an appropriate ethical and legal framework for AI technology and applications. New draft guidelines have been proposed and Hogan Lovells was asked to submit a paper to the European Commission commenting on those draft guidelines.



Valerie Kenyon
Partner, London Office
T + 44 (20) 7296 5521
valerie.kenyon@hoganlovells.com



The effects of rapid technological change on US regulatory policies in the communications sector

Predicting what future changes in technology may occur is often an impossible endeavor. Designing effective regulatory policies around changing technologies is even more difficult, as it requires understanding how those changes may alter market conditions that often render such policies obsolete or even counterproductive. Robert W. Crandall, together with T-Mobile and Hogan Lovells, have prepared a report providing a detailed critique of four US regulatory policies involving telecommunications, media and cable television that were overtaken by technological change that rendered these policies unnecessary or even counterproductive. The report demonstrates that in industries characterized by rapid technological change, regulation often leads to counterproductive constraints on firms, which are hard to lift and stay in place for a long time. Crandall says that regulators should be particularly cautious in intervening in the changing telecommunications market. In this issue we include an extract from the report on the artificial distinction between "local" and "long-distance" calling in telecommunications regulation. To read the full report, visit <https://bit.ly/2CVlhqz>.

The artificial distinction between "local" and "long-distance" calling in telecommunications regulation

In the modern digital age, one may communicate with others through a wireless or wireline telephone call, a text message, an e-mail, or through a social media site. The price of using any of these media for such a communication is rarely distance sensitive and may be zero or close to zero in many cases. The distance insensitivity of communications prices is a rather recent phenomenon, one driven by changes in technology and – belatedly – by changes in regulatory policies.¹

In the earliest days of telephony, the average cost of transmitting a signal varied with distance because of the technology employed. At first, signals were transmitted only over copper wires. The cost of sending a call over such facilities rose substantially with distance. After World War II, microwave technology began to replace copper wires, reducing the cost of transmitting "long distance" calls, but not eliminating the distance sensitivity of the cost of calls. Once fiber optics began to displace microwave as the dominant technology in long-distance transmission, the cost of transmitting calls across hundreds or even

“

“As long-distance costs fell due to technological change, this artificial regulatory distortion of the relative prices of interstate and intrastate services grew.”

”

thousands of miles declined dramatically. Today, the full cost of transmitting a call from New York City to, say, Los Angeles might still be somewhat above the cost of transmitting it to Newark, NJ, but the differences in transmission cost are so small that they are likely not worth measuring and billing consumers for them.

Regulatory price distortions

Prior to the entry of new long-distance carriers in the 1960s, federal and state regulators controlled the telephone rates of AT&T, the dominant U.S. carrier, and various smaller companies. A Joint Board of these regulators made recommendations to the Federal Communications Commission (FCC) on the allocation of carriers' costs between intrastate and interstate jurisdictions. In an effort justified as necessary to achieve “universal service,” these regulators allocated a substantial share of the fixed (non-traffic-sensitive) costs of the telephone network to interstate long-distance calls, even after the cost of such calls had begun to decline rapidly with the introduction of microwave transmission.ⁱⁱ

The result of this allocation of costs was to elevate interstate long-distance rates relative to costs so as to keep local telephone rates correspondingly low. As long-distance costs fell due to technological change, this artificial regulatory distortion of the relative prices of interstate and intrastate services grew.

The 1974 U.S. v. AT&T antitrust case was settled by a consent decree in 1982, which provided for vertical divestiture of AT&T's local operating companies.ⁱⁱⁱ This divestiture was completed in 1984. AT&T continued as a long-distance carrier, competing with new carriers such as MCI, Sprint, and WorldCom, and its local operations were spun off to seven Region Bell Operating Companies. The vertical separation of local and long-distance wireline service required the FCC to set explicit access charges that the divested operating companies would charge AT&T and other long-distance companies for originating and terminating their interstate calls.

Were the access charges to be established at levels that preserved the pre-divestiture rate structure, they would have to be very high. Indeed, they were initially set at more than 17 cents per conversation minute. Realizing that these access charges were far above any reasonable estimate of costs, the FCC began to reduce them, substituting a monthly fixed “subscriber line charge” that residences and businesses would pay on their local telephone bills to rebalance rates towards their relative costs and allow the local carriers to recover the lost revenues. See Table 1.

Between 1984 and 2004, per-minute access charges were reduced steadily from 17.3 cents to 1.4 cents while the subscriber line charge for residences and single-line businesses rose from \$0 to \$5.96 per month and the subscriber line charges for multi-line

“

“The rebalancing of rates after the AT&T divestiture was the major force in driving down interstate long-distance rates.”

”

businesses rose to more than \$6 per month.^{iv} These dramatic changes in the telephone rate structure following the AT&T divestiture were phased in over nearly two decades in order to avoid an adverse public reaction from those most affected by a rise in the fixed cost of subscribing to the telephone network – the flat local rate plus the subscriber line charge – even if those rates more accurately reflected costs.^v The average price of a local residential line rose from \$15.18 per month in 1984 to \$24.52 in 2004 while the average price for interstate and international calls fell from 32 cents per minute to 8 cents per minute over the same period.^{vi} Note that the decline in interstate access charges over this period accounted for nearly 16 cents of the 24 cents-per minute decline. Thus, the rebalancing of rates after the AT&T divestiture was the major force in driving down interstate long-distance rates.

The continuation of FCC regulation despite the increase in competition from new technologies

As far back as 1974, the FCC began to develop its policy of licensing the electromagnetic spectrum for mobile wireless services.^{viii} The first U.S. cellular service began operating in 1983 using an analog technology. The demand for the new service was substantial as reflected in the rapid growth in cellular subscriptions. By 1988, there were more than 2 million subscribers; by 1993, just ten years after the introduction of cellular service, 16 million subscribers had cellular handsets;^{ix} and by 2016, subscriptions totaled 396 million.^x

In 1998, AT&T Wireless announced a new Digital One Rate plan that allowed subscribers to call anywhere in the United States for the same price, a price that declined with overall minutes of use in the chosen variant of the plan.^{xi} Soon, other carriers began offering similar pricing plans, and subscribers responded

Table 1
The Federal Communications Commission's Rebalancing of Wireline Telephone Rates 1984-2004

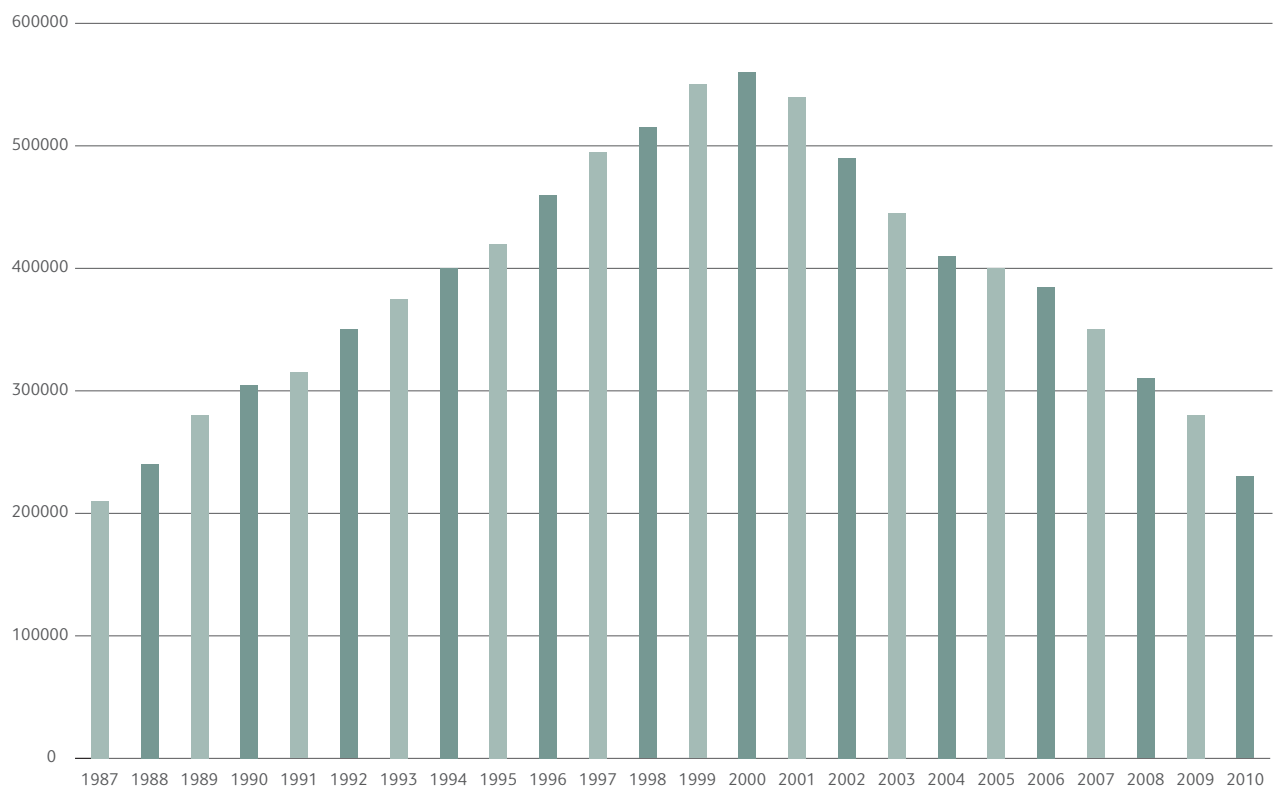
| Period | Residential and Single-Line Business Subscriber Line Charge (\$/mo.) | Multi-Line Business Subscriber Line Charge (\$/mo.) | Interstate Switched Access Charge per Conversation Minute (¢/min.) |
|------------------|--|---|--|
| 5/26/84-1/14/85 | 0.00 | 4.99 | 17.26 |
| 1/15/85-5/31/85 | 0.00 | 4.99 | 17.66 |
| 6/01/85-9/30/85 | 1.00 | 4.99 | 16.17 |
| 10/01/85-5/31/86 | 1.00 | 4.97 | 15.38 |
| 6/01/86-12/31/86 | 2.00 | 4.97 | 14.00 |
| 1/01/87-6/30/87 | 2.00 | 5.12 | 12.41 |
| 7/01/87-12/31/87 | 2.60 | 5.12 | 11.49 |
| 1/01/88-11/30/88 | 2.60 | 5.01 | 10.56 |
| 12/01/88-2/14/89 | 3.20 | 5.01 | 9.60 |
| 2/15/89-3/31/89 | 3.20 | 5.01 | 9.46 |
| 4/01/89-12/31/89 | 3.50 | 4.94 | 9.11 |
| 1/01/90-6/30/90 | 3.48 | 4.84 | 7.78 |
| 7/01/90-12/31/90 | 3.48 | 4.83 | 7.48 |
| 1/01/91-6/30/91 | 3.48 | 4.77 | 7.18 |
| 7/01/91-11/27/91 | 3.49 | 4.74 | 6.97 |
| 11/28/91-6/30/92 | 3.49 | 4.76 | 6.97 |
| 7/01/92-6/30/93 | 3.49 | 4.68 | 6.76 |
| 7/01/93-6/30/94 | 3.50 | 5.37 | 6.66 |
| 7/01/94-6/30/95 | 3.50 | 5.45 | 6.89 |
| 7/01/95-6/30/96 | 3.50 | 5.50 | 6.16 |
| 7/01/96-6/30/97 | 3.50 | 5.53 | 6.04 |
| 7/01/97-12/31/97 | 3.50 | 5.68 | 5.18 |
| 1/01/98-6/30/98 | 3.50 | 6.92 | 4.04 |
| 7/01/98-12/31/98 | 3.50 | 7.11 | 3.82 |
| 1/01/99-6/30/99 | 3.50 | 7.05 | 3.71 |
| 7/01/99-12/31/99 | 3.50 | 6.94 | 2.82 |
| 1/01/00-6/30/00 | 3.50 | 6.94 | 2.85 |
| 7/01/00-6/30/01 | 4.28 | 6.88 | 1.91 |
| 7/01/01-12/31/01 | 4.78 | 6.66 | 1.71 |
| 1/01/02-6/30/02 | 4.92 | 6.79 | 1.69 |
| 7/01/02-6/30/03 | 5.62 | 6.45 | 1.46 |
| 7/01/03-6/30/04 | 5.96 | 6.37 | 1.44 |

Source: 2011 Monitoring Report, Tables 4.4 and 4.5. FCC.^{vii}

by using their cellular phones to make long distance calls that they had been making over their traditional wireline connections because the wireless calls did not incur traditional wireline access charges and were cheaper. The result was a dramatic shift of long-distance calling from traditional wireline to wireless carriers. Moreover, in 2003 cable television companies began to offer distance-insensitive Voice over Internet Protocol (VoIP) calling services. These competitive developments induced a sharp decline in interstate switched access minutes reported by local wireline carriers, as shown in Figure 1.

Despite the rapid growth of wireless telephony, the FCC continued the regulation of wireline carriers. The 1996 Telecommunications Act (“1996 Act”) established a detailed policy of requiring that the dominant, incumbent wireline carriers – principally the Bell Operating Companies that were divested by AT&T in 1984 – allow competitors to lease portions of their networks at regulated wholesale rates. These wholesale rates were set by state regulators under guidelines established by the FCC. In addition, the FCC had the responsibility of regulating interstate long distance rates and ruling on a variety of issues that arose under the 1996 Act. All of this regulation continued despite the obvious growth of competition from wireless providers in the late 1990s.

Figure 1
Interstate Switched Access Minutes, Local Wireline Carriers, 1987-2010



Source: 2012 Monitoring Report, Chart 5.1, FCC.^{xii}

As early as 2001, the FCC offered the following observations about the growth of wireless competition:

According to a recent survey by the Yankee Group, about 3 percent of mobile telephone subscribers rely on their wireless phone as their only phone. While most wireless customers may not be willing to “cut the cord” just yet in the sense of canceling their subscription to wireline telephone service, it is indisputable that wireless service has significantly changed the way Americans communicate. Initially a business tool, wireless phones have become a mass-market consumer device. According to one survey, 77 percent of wireless customers said they use their phones primarily for personal calls. For some, wireless service is no longer a complement to wireline service but has become the preferred method of communication. In a survey performed for the Consumer Electronics Association, three in 10 wireless phone users stated they would rather give up their home telephone than their wireless phone. Among wireless users aged 18 to 34 years old, that figure rose to 45 percent.^{xiii}

Thus, the FCC recognized that wireless communications were competing strongly with wireline services very soon after AT&T introduced its Digital One Rate plan in 1998. Nevertheless, the FCC and state regulators continued their regulation of the wireline carriers and long-distance service.^{xiv}

It was already becoming clear by 2001 that the competitive landscape had changed. The long-distance carriers, principally AT&T and MCI, would never enter the market for local wireline service in a meaningful way and their long-distance service businesses were declining rapidly. In

“

“Regulators should be cognizant of the difficulties their predecessors faced in dealing with dramatic changes in technology and unwinding inefficient regulations.”

”

2005, AT&T agreed to be acquired by Southwestern Bell and MCI was acquired by Verizon. The viability of standalone long-distance carriers had been undermined by competition from wireless service and VoIP providers. The major focus of regulatory policy finally turned away from “local” and “long distance” voice services to Internet broadband services but this occurred 30 years after the FCC first announced a policy of allocating spectrum for cellular wireless services, 22 years after the first cellular service was launched in the United States, and 12 years after Congress authorized spectrum auctions.

Nevertheless, the FCC and state regulators continue to regulate traditional wireline services, largely in an effort to continue to promote “universal service.” Technological change has clearly eliminated the original case for the detailed regulation of telephone rates as wireless services and VoIP have become available to virtually all consumers, but regulation continues because of the apparent political appeal of using the FCC’s regulatory authority as a mechanism for taxing^{xv} consumers of interstate and international telecommunications services for the benefit of rural carriers, schools, libraries and rural health facilities. The technological revolution driving wireless telecommunications today is more dramatic and fast-paced than the changes which occurred between the AT&T divestiture and 2005. Regulators and antitrust authorities should therefore be cognizant of the difficulties their predecessors faced in dealing with dramatic changes in technology and unwinding inefficient regulations between 1984 and 2005.

The adverse effects of FCC regulation on economic welfare

For decades before the Department of Justice brought its antitrust suit against AT&T in 1974, the FCC and the states had operated a policy of keeping the monthly subscriber charge for telephone service below cost and compensating the carriers – principally AT&T – for the loss in revenues by establishing high rates for calling, particularly over long





distances. In brief, this was a policy that made it inexpensive for consumers to have a phone but unduly expensive to use it. Such a policy reduces the value of telephone service to producers and consumers because the demand for telephone connections (local service) is far less price sensitive than the demand for long-distance usage. As a result, this policy provides very small increases in telephone subscriptions, but much greater decreases in (long-distance) usage.

In *Who Pays for Universal Service? When Telephone Subsidies Become Transparent*, Crandall and Waverman estimated that the total economic welfare loss due to the regulatory mispricing of residential telephone service in 1996, long after the FCC had begun to rebalance rates, was still between \$2.5 billion and \$7 billion per year, depending on the assumed marginal cost of long-distance service and the cost model used to determine the cost of local service.^{xvi} These estimates would have been much higher if the rate structure had been the one that existed before the FCC began to rebalance rates in 1984 after the AT&T divestiture. By 1996, residential subscribers were paying a \$3.50 per month subscriber line charge, which would allow long-distance rates to be 2.5 cents per minute lower, all other factors being constant. Had the FCC not imposed this subscriber line charge, the welfare loss due to mispricing would have been as much as \$2 billion more – or as much as \$9 billion per year in 1996.^{xvii}

The annual cost of this regulatory price distortion was very high for years – if not decades. Equally important, empirical studies of this “universal service” policy consistently show that this policy has little effect on overall telephone subscriptions because artificially low local rates can only induce additional subscriptions from the very few households that do not already subscribe.^{xviii} On the other hand, everyone’s long-distance rates are raised by the policy.

Had the FCC moved more aggressively to introduce cellular wireless services after its spectrum allocation decision in 1975, competitive pressures from wireless services would likely have begun much sooner. Such competition may have made the 1996 Act unnecessary and would have thus spared the country the ill effects of another decade of misguided regulation.

Robert W. Crandall

Robert W. Crandall is an adjunct senior fellow at the Technology Policy Institute. His current research focuses on antitrust and regulatory issues in the telecommunications sector. He is the author or coauthor of numerous articles and books and communications policy. Crandall is also a nonresident senior fellow in the Economics Studies program at the Brookings Institution. He has also served as a consultant to the Antitrust Division, the Federal Trade Commission and the Treasury Department.

A game changer? China enacts first e-Commerce Law



On 31 August 2018, the Standing Committee of the National People's Congress ("NPC") passed China's first law regulating electronic commerce, the People's Republic of China e-Commerce Law ("e-Commerce Law"). The new law will enter into force on 1 January 2019.

Legislative work for the new, hotly debated law started as far back as in December 2013, and since then, no less than four drafts have been submitted to the NPC for review (several of which were commented on by the public, e.g. see here for our alert on the second draft). This long drawn out process and unusually large number of drafts point to the protracted battles that have taken place behind the scenes between the various stakeholders in this space.

The professed aim of this new law is to regulate China's rapidly growing e-commerce sector, harmonize its rules with those applicable to brick-and-mortar shops, maintain "market order," facilitate growth, and eradicate IP infringements, scams and unfair competition.

Reading between the lines, the real aim of the e-Commerce Law is to try and bring some order to what has become a hugely successful, but somewhat unruly sector of the Chinese economy. If you want evidence of the runaway success story that is the China e-commerce market, you need look

no further than the last Singles Day (11 November), a sort of anti-Valentine's Day shopping binge in which Alibaba reportedly made a record US\$25 billion in sales on the day, a 40% increase on the previous year, involving 140,000 brands, 15 million products, 12 million orders, and 1.48 billion payments processed. US Black Friday and Cyber Monday in 2016, the nearest rough comparable, generated a mere US\$6.79 billion in sales.

On the other hand, if you want evidence of how some less scrupulous online operators have scammed, imposed egregious terms on consumers, or otherwise violated consumers' rights, you need look no further than the huge volume of cases blocking up the Chinese courts. There is, however, no way back now, and online shopping and precariously balanced piles of parcels ready for delivery engulfing electric scooters have become so much a part of the landscape in major cities in China, that they tend to fade into the background.



Scope

One of the most striking features of the new e-Commerce Law is its broad scope (Article 2): the law is applicable to all e-commerce activities taking place within the People's Republic of China. e-commerce is broadly defined as the sales of goods or services through the internet or any other information network. Some activities, such as the provision of financial products and services, news, audio or video programs, publication and cultural services are excluded from the scope of the law. Presumably these are sensitive products which will be separately regulated.

The law specifically regulates the conduct of three main types of e-commerce operators (Article 9):

- platform operators (e.g., the large Chinese e-commerce platforms such as Taobao or JD.com)
- in-platform operators (e.g., individual e-shops active on those platforms, such as sellers who have T-Mall shops), and
- other operators who conduct their e-commerce business through their own websites or any other network services (e.g., websites of bricks and mortar traditional retailers or those who trade through public accounts on instant messaging apps).

This means that the new law is applicable to both the 'traditional' e-commerce operators (e.g. those active on platforms) and non-traditional e-commerce operators (e.g., those who operate their business through apps).

Business licenses and taxation

One of the more controversial provisions introduced in the second draft of the law has made it into the final version of the law: in principle, all e-commerce operators have to obtain a business license (Article 10). Exceptions to this requirement are only made for providers of certain agricultural by-products, cottage industry products, services to benefit the public, and low-value intermittent transactions.

Moreover, all e-commerce operators have to issue "fapiao" (official tax receipts) and file tax returns (Articles 11 and 14), even those that are exempt from obtaining a business license. The new law explicitly recognizes that electronic invoices have the same legal value as hard-copy tax receipts.

This is a significant and hotly debated change, given the fact that currently small in-platform operators and operators active on social networks often de facto do not need to apply for a business license or file tax returns. The argument in favour of this change is that the online and the offline industries should be subject to the same rules on administrative permits and taxation, and consumers need a minimum level of protection from unscrupulous unregistered operators who can disappear without a trace.

In order to ensure that all in-platform operators obey these rules, the new law obligates platform operators to conduct true identity checks, to verify business licenses and to submit identification and tax information to the tax authorities (Articles 27-28).

e-commerce advertising

The new law reiterates some of the prohibitions under the People's Republic of China Advertising Law, but tailors them to an online setting: e.g. it is forbidden to fabricate false transaction information, produce false user reviews, delete genuine user reviews and sponsored listings should be clearly marked as such (Articles 17 and 40). The law also contains a general prohibition on misleading and defrauding consumers (Article 17). Moreover, there is an important development tracking China's broader moves towards more comprehensive data protection regulation. e-commerce operators must give consumers the choice as to whether or not they wish to have their search results personalized based on their identifiable traits, personal interests and so forth (Article 18). This will require some search operators to reconfigure their systems.

Antitrust references

The e-Commerce Law touches upon antitrust issues, without however adding substantially to the existing legal framework laid out by the People's Republic of China Anti-Monopoly Law ("AML"). For instance, Article 22 of the e-Commerce Law prohibits abuses of a dominant market position. But the provision seems to merely act as a reference back to the AML, since the e-Commerce Law itself does not provide any sanctions for non-compliance. The only new content relative to the AML is that Article 22 sets out a few factors that may help identify a dominant market position for e-commerce players, namely technological superiority, user numbers, control over the industry or dependence by other businesses on transactions with the player in question.

Furthermore, Article 19 prohibits hidden tie-in activities, for example through tying products or services by default mechanisms. Here, the e-Commerce Law departs from the AML, as it does not require the company at issue to be in a dominant position as a starting point. The same is true for the prohibitions upon online sellers and platforms on imposing unreasonable conditions on consumers (Articles 21 and 35).

Intellectual property

The new law provides, in Articles 41-45, a formal framework and detailed rules for the notice-and-take-down procedures that already exist in some form under the existing laws/regulations (e.g. the People's Republic of China Tortious Liability Law) which many major e-commerce platforms have already adopted in China.

Under the new law, e-commerce platform operators must provide for contradictory notice-and-takedown procedures – somewhat similar to the notice-and-take down procedures under the US Digital Millennium Copyright Act. This means that an IP owner can file an infringement notice with an e-commerce platform, requesting "necessary measures", such as deletion, blocking or disconnection of links and termination of transactions and services of an infringing in-platform operator (Article 42). Such takedown notice must include prima facie evidence of the infringement (we anticipate further implementation rules and judicial guidance on the level of prima facie evidence required). The e-commerce platform must then take appropriate measures (e.g. removing the postings



or blocking links to allegedly infringing products etc.) and must forward the notice to the in-platform operator.

The in-platform operator may, in turn, file a notice of non-infringement, which must also include prima facie evidence of non-infringement (Article 43). The platform operator has to forward such notice to the complainant, and must advise that the complainant has to lodge a formal complaint with the authorities or bring suit before court. If no such action follows within 15 days, the platform operator must lift the measures it has adopted.

The new law also contains detailed provisions on liability for IP infringements (Articles 42 and 45). Platform operators that do not take timely and appropriate measures after a notice-and-takedown procedure shall be held jointly and severally liable for additional damages caused by prolonged IP infringement. Platform operators that knew or should have known about IP infringements on their platform are held jointly and severally liable with the infringers. On the other hand, IP owners who erroneously or maliciously initiate a takedown will have to compensate the e-commerce merchants.

Division of liability between platforms and in-platform operators

The e-Commerce Law prescribes a division of liability between platform operators and in-platform operators (Article 38).

On the one hand, the new law provides that a platform operator who knows or should know about defective or harmful products or services being listed on its platform, but who nevertheless fails to take the necessary measures, will be held jointly and severally liable with the infringing in-platform operator.

On the other hand, in respect of goods or services that affect the life and health of consumers (e.g. medical products or treatments), if a platform operator fails to examine the qualifications of its in-platform operators or fails to protect its consumers' safety, then the platform operator and the in-platform operator must assume their "corresponding liability" towards impacted consumers. The terminology is vague and is capable of numerous interpretations: the simplest of these is that each assumes liability based on its respective degree of fault. A more complicated scenario would be that where the platform operator has not done its due diligence – would it assume either (a) joint and several liability with the in-platform operator; or (b) just the shortfall to the extent not paid by the in-platform operation? It appears that the wording is something of a 'fudge', leaving the courts to determine what it actually means. This is a significant change from the third draft of the law, which imposed joint and several liability on platform operators in these situations. This change is widely seen as favouring platform operators rather than consumers. The sensitivity of this area no doubt stems to some degree from the tragic 2016 case of a Chinese student who died after undergoing experimental therapy which came out high in the rankings of a local search engine, which generated a significant public debate in China about the ethics and duties of operators of search engines.

“

“One of the most controversial aspects of the new law is the obligation for individual web shops on e-commerce platforms to obtain a business license and pay taxes.”

”

Data protection and cybersecurity

The new e-Commerce Law emphasizes personal information protection and contains several provisions regarding the treatment of personal information of e-commerce users (Article 24): the law introduces a duty for e-commerce platforms to explain how data is gathered and searched. Moreover, similar to EU data protection law, users also enjoy the right to enquire about, correct or delete any of their personal information saved by e-commerce operators, or to deregister altogether.

Continuing the course of a gradual broadening of data protection laws in China, including under consumer rights rules and as encouraged under the new Information Security Technology – Personal Information Specification introduced in May, 2018, the new law requires e-commerce platforms to adopt technical or other measures to protect network security and adopt contingency plans for cybersecurity incidents (Article 30). If a platform's cybersecurity is compromised, it must immediately activate its contingency plan and report the incident to the authorities. In addition, the new law specifically requires that the platform operators must submit relevant e-commerce business data and information when the administrative authorities make such a request in accordance with applicable laws and regulations (Article 25).

These provisions are generally consistent with those in the People's Republic of China Cyber Security Law.

See also how this parallels China's moves to require disclosure of scientific data.

The Cyber Security Law and its supporting rules do not include a specific period requirement for data retention (except for the 6-month retention period requirement for web logs). While the new e-Commerce Law requires that platform operators keep the product and service information and transaction information for no less than 3 years and must ensure the completeness, confidentiality and utilization of such information (Article 31). This retention period is in line with the statute of limitation for civil lawsuits stipulated in the new People's Republic of China General Civil Law Rules, effective 1 October 2017.

Shipment risks and liabilities

Under the new e-Commerce Law, e-commerce operators must deliver goods or services to consumers in accordance with what was promised and in the manners or at the time agreed with consumers, and assume the risks and liabilities during the shipment of goods, unless consumers reach an agreement with e-commerce operators to select another logistics service provider (Article 20). This is in line with current practice with major e-commerce operators in China, so confirms market practice.

e-commerce complaints

The new law provides that e-commerce operators must set up straightforward and effective complaint and reporting mechanisms, disclose complaint and reporting channels, and must accept and handle any complaints in a timely manner (Article 59). This aims to address the challenges that consumers may encounter at the time they seek to enforce their rights as consumers.

Sanctions

The new law provides for a range of sanctions for infringements (Articles 74-88). However, the monetary thresholds are generally quite low given the volumes and turnover of the major operators. The maximum penalty is RMB 2 million (around US\$300,000) for serious violations such as e-commerce platform operators unreasonably restricting or attaching unreasonable conditions on transactions or transaction price charged by in-platform operators, or platform operators who fail to take necessary steps against in-platform operators who infringe upon rights of consumers or fail in their obligation to review the qualifications of in-platform operators. Most violations are punished by fines between RMB 20,000 and 500,000 (around US\$3,000 to 75,000), which are not high amounts, especially for large platform operators. In addition to imposing from monetary sanctions, the new law also prescribes that any infringement of the law will be registered in the infringer's creditworthiness file.

Conclusion

The e-Commerce Law is, all-in-all, largely a reflection of existing practice, but also aims to eliminate some of the more egregious forms of online commercial behaviour. It is a delicate and difficult balancing act, and only time will tell whether the right balance has been struck between all the stakeholders who will all, no doubt, have expressed strong views on how their interests needed protection. It does mean that consumers now have a more comprehensive, single-source set of rules governing the online space, to fill out the piecemeal provisions in, for example, the recently updated People's Republic of China Law on the Protection of Consumer Rights and Interests, but it does point to the need for the People's Republic of China Contract Law to undergo an overhaul to reflect the quantum shift towards online transactions since it came into effect on 1 October 1999.

The issue is whether it is still possible to put the genie back in the bottle, the dragon back in the castle (or any other metaphor you care to use) to describe the fact that it is astonishing that we have had to wait until 2018 for the first dedicated law to regulate the largest e-commerce market on the planet (by a country mile).

The focus of the new e-Commerce Law is also firmly on domestic e-commerce, and there is not much in the way of detail on how cross-border e-commerce will be regulated. There are lots of fine words in terms of the State encouraging the development of infrastructure for cross-border e-commerce and information sharing and mutual recognition of regulation and assistance in law enforcement, but China has yet to agree a set of mutual assistance and recognition of judgments agreements or treaties with many of its key trading partners (other than Hong Kong,

“

“Consumers now have a more comprehensive, single-source set of rules governing the online space.”

”



which is limited in scope), and the current trade tensions with the US and protectionist tendencies do not provide a favourable backdrop for this to happen.

There is a clear duality to many of the provisions, depending on which side of the fence you sit. One of the most controversial aspects of the new law is the obligation for individual web shops on e-commerce platforms to obtain a business license and pay taxes. It may put many smaller players out of business or force them underground, so is seen as quite harsh in some quarters. However, this new obligation could have a markedly positive impact for IP owners, as it would make it harder for bad-faith IP infringers to evade enforcement actions by IP owners by simply closing their web shop (or having it taken down by the platform) and opening a new one.

It is that duality that presumably made it so hard to reach consensus on the wording of the e-Commerce Law in the first place.



Roy Zou
Partner, Beijing Office
T + 86 (10) 6582 9596
Email: roy.zou@hoganlovells.com



Andrew McGinty
Partner, Shanghai Office
T + 86 (21) 6122 3866
Email: andrew.mcgintry@hoganlovells.com



Adrian Emch
Partner, Beijing Office
T + 86 (10) 6582 9510
Email: adrian.emch@hoganlovells.com



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




Sherry Gong
Counsel, Beijing Office
T + 86 (10) 6582 9516
Email: sherry.gong@hoganlovells.com



Mark Parsons
Partner, Hong Kong Office
T + 852 2840 5033
Email: mark.parsons@hoganlovells.com

Using contracts to manage AI risk



Many firms, including those that do not regard themselves as traditional “tech” firms, consider the prospect of artificial intelligence (AI) both an intriguing possibility and a potential new area of risk for their businesses. They want to make sure they can seize the new opportunities and manage the new risks that AI promises. Yet achieving these objectives can be particularly challenging, given that firms face uncertainties concerning the current and future state of AI technology and when and how it will significantly impact them. Hogan Lovells partners Jason D. Lohr, Winston J. Maxwell and Peter Watts have written a chapter entitled “Legal Practitioners’ approach to regulating AI risks” to appear in K Yeung and M Lodge (editors) *Algorithmic Regulation*, Oxford University Press 2019 (forthcoming), examining how businesses are already managing some of these risks through contract. They also examine some of the considerations involved in public regulation of AI-related risks. In this issue we include an extract from their chapter.

The application of existing AI technologies raises significant new issues in some of the most fundamental areas of law, including: ownership and property rights; the creation, allocation and sharing of value; misuse, errors and responsibility for resulting harm; individual liberty and personal privacy; economic collusion and monopolies. In principle, many AI-related risks should be capable of being managed through legally binding contracts – for example, between the business providing an AI tool and its enterprise customers who use the tool, between the enterprise user and its insurers, and between the enterprise user and its customers. But in practice, businesses (and insurers, investors and consumers) are faced with the need to develop new approaches to contracts to address these developing risks whilst those risks continue to evolve.

AI systems involve at least three stakeholders in the vertical value chain: the developer of the AI system, the enterprise customer, and the end-user (which may be the customer's customer). The contracts between the AI system developer and the enterprise customer will be the first important risk mitigator.

“

“The contracts between the AI system developer and the enterprise customer will be the first important risk mitigator.”

”

Protecting the value of a trained AI model

Development of machine learning tools is a significant investment. Developers (and their investors) will want to ensure that they secure the value in their tools. The discussion in this section identifies various ways in which contractual risk management techniques can be adopted in order to protect the value of this investment, from the perspective of developers and their investors. Like other software tools, most trained machine learning models will contain elements which are capable of protection as copyright, patent or other intellectual property. Those concerned to protect their investment in these models should ensure that ownership or usage is clearly specified in agreements and licenses, with pricing set accordingly.

The enterprise whose data is teaching the model will wish to protect the value of its data through appropriate contractual restrictions. While the intellectual property rights associated with raw data are not always clear, enterprises holding data generally have the right to restrict usage. Where personal data are involved, imposing contractual restrictions on use is an obligation in some legal systems.^{xix}

The legal treatment of any models trained by using that data (in particular whether a trained model will be protected as intellectual property) is less clear. Nonetheless, enterprise users wishing to retain rights to those models regardless of the entity doing the training could attempt to do so via contract. Even for enterprise users not seeking to retain ownership of trained models, it may be wise for them at least to define or restrict the usage of the trained model, at least for certain industries or with respect to other competitors. If the training will involve data from multiple entities, as in the case of big data consortium projects for example, this may include specifying the scope for which each of the consortium members may utilize the trained models, or results produced by those models.

In addition to these protective provisions concerned with protecting the value of a firm's investment in AI tools, firms at each stage of the chain of origination, development and use of machine learning tools, including data providers and technology developers, commercial considerations may affect the way in which their relationships are legally structured. For example, should their relationships be based on a royalty type model (e.g. percentage of revenues generated) rather than a flat fee? If so, what provisions need to be included to ensure that the revenues used as the basis for the royalty calculation reflect all of the value generated? Should the relationship be structured as a consortium or joint venture? Should there be co-ownership in the trained model or results? Should a separate entity be created to conduct the analysis and control access to the results?



Contractual use restrictions to avoid revealing trade secrets

The training of the machine learning algorithms may enable others to learn trade secrets or patentable technology. To prevent this, it might be appropriate to restrict the usage of the machine learning model to prevent use for any application or entity that might gain advantage from such trade secrets or technology.

It might also be possible to restrict certain types of decisions from being made using the trained machine learning algorithms, where those decisions may relate to the defined intellectual property.

The training data, trained models, and usage thereof should also be analyzed to determine whether they themselves constitute trade secrets or patentable subject matter requiring legal protection.

Specific provisions may also be included in commercial agreements to indicate the ownership of any inventions utilizing, or resulting from usage of, the trained machine learning models or results.

Allocating liability if things go wrong

A key contractual question will be the allocation of liability for decisions made using machine learning. This might be anything from harm caused to a patient who is wrongfully diagnosed by a tool, to injury to a pedestrian who is not accurately identified by an autonomous driving system, to a wide range of financial losses which businesses might suffer from “errors” made by AI tools. The various businesses involved in the development and deployment of machine learning tools (and their insurers) will want to allocate liability risks so that it is clear who is responsible if something goes wrong. The law has a well-established framework for identifying when civil liability arises. For example, the law of negligence generates obligations of compensation if proper care has not been taken. The main tools available for that allocation between businesses will be contractual promises by which one party agrees to assume liability to another (typically warranties and indemnities) and agreements to limit the liability of one party to another. Firms exposed to potential civil liability associated with the use of AI tools will understandably wish to employ contractual risk management approaches to allocate liability to the entity in the best position to prevent the harm in the first place. They will also wish to ensure that the ways they have traditionally used contractual risk management will function as intended when faced with new scenarios.

One example of a new scenario in which machine learning will generate potential liabilities which will need to be addressed is where one entity provides training data to enable development of a tool. That entity may be liable for the accuracy of that training data, including any labeling or classification data that is relied upon, so that if use of the trained model “harms” someone the provider of the data could have legal responsibility for that harm. This potentially generates a need for indemnification

to make clear who will bear the costs arising from any inaccurate or improper training data. Similarly, if an entity provides a trained model for a specific purpose (distinguishing a human from a shadow on the road for example), that entity may need to provide indemnification for decisions made by the trained model where those decisions are utilized to perform an action that results in injury to person or property (such as a pedestrian struck by an autonomous vehicle equipped with that tool). Equally, they will want to seek an indemnity from anyone purchasing the tool against the consequences of it being used other than for the purposes for which it has been designed.

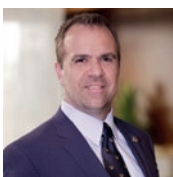
Firms may also wish to make provision requiring some type of auditing to enable them to verify the provenance of the tool. This might require that information as to the process or logic used to make specific decisions will be available and maintained for at least a minimum period of time. Provisions of this type might also include determining the type of information to be made available for auditors.

As discussed above, in some instances machine learning models may learn relationships that are not easily explainable in human terms, but produce very accurate results. A consideration may be made as to whether to specify that the machine learning should be limited to explainable decisions or relationships only, even though it may result in somewhat less accurate decisions or results, specifically where there are significant liability or regulatory issues that require a full audit trail.

“

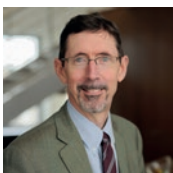
“A key contractual question will be the allocation of liability for decisions made using machine learning.”

”



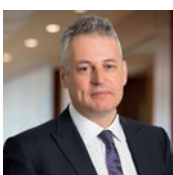
Jason Lohr

Partner, San Francisco, Silicon Valley
 T +1 415 374 2339 (San Francisco)
 +1 650 463 4152 (Silicon Valley)
 Email: jason.lohr@hoganlovells.com



Winston Maxwell

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



Peter Watts

Partner, London
 T +44 20 7296 2769
 Email: peter.watts@hoganlovells.com

References

- i. For a thorough discussion of this development, see FRANCES CAIRNCROSS, *THE DEATH OF DISTANCE: HOW THE COMMUNICATIONS REVOLUTION IS CHANGING OUR LIVES* (2001).
- ii. The non-traffic-sensitive costs allocated to the interstate jurisdiction were recovered on a usage-sensitive basis with charges levied for each call on the basis of time and distance. For a description of this policy, see ROBERT W. CRANDALL AND LEONARD WAVERMAN, *WHO PAYS FOR UNIVERSAL SERVICE? WHEN TELEPHONE SUBSIDIES BECOME TRANSPARENT* (2000).
- iii. *See Modification of Final Judgment, U.S. v. American Tel. and Tel. Co.*, 552 F. Supp. 131 (D.D.C. 1982), *aff'd. sub. nom., Maryland v. U.S.*, 460 U.S. 1001 (1983).
- iv. *See Universal Service Monitoring Report*, FCC, at Tables 7-12 and 7-13 (June 1999), <https://www.fcc.gov/general/monitoring-reports-2010-and-earlier>.
- v. This rebalancing did not result in fully cost-based pricing.
- vi. *See Trends in Telephone Service*, Report, DOC-301823, Tables 13.3 and 13.4 (Sept. 2010).
- vii. *See Universal Service Monitoring Report*, Report, DOC-311775 (Dec. 29, 2011).
- viii. *See Inquiry Relative to the Future Use of the Frequency Band 806-960 MHz, Amendment of Parts 2, 18, 21, 73, 74, 89, 91, and 93 of the Rules Relative to Operations in the Land Mobile Service Between 806-960 MHz*, Memorandum Opinion & Order, 51 FCC 2d 945 (1975).
- ix. *See Trends in Telephone Service* at Table 11.3.
- x. *See Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services*, Twentieth Report, 32 FCC Rcd 8968 ¶ 5 (2017).
- xi. *See Cell Phone Plan Debuts*, CNN MONEY (May 7, 1998), <https://money.cnn.com/1998/05/07/technology/attwireless/>.
- xii. *See Universal Service Monitoring Report*, Report, DOC-319744 (Mar. 22, 2013).
- xiii. *See Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Commercial Mobile Services*, Sixth Report, 16 FCC Rcd 13350, 13381 (2001) ("Sixth Mobile Competition Report").
- xiv. The FCC declared AT&T "non-dominant" in the provision of long distance services in 1995, thereby eliminating detailed regulation of its interstate rates. *See Motion of AT&T Corp. to be Reclassified as a Non-Dominant Carrier*, Order, 11 FCC Rcd 3271 (1995). AT&T still had to file interstate tariffs that were just, reasonable and non-discriminatory. The FCC continued to regulate the interstate carrier access charges paid by long-distance carriers to local carriers, and the states continued their regulation of intrastate long distance service rates.
- xv. Considerable controversy has existed over whether the federal universal service charge should be defined as a "tax," but it clearly is a government-imposed charge imposed on consumers of interstate and international telecommunications services – in effect, a tax.
- xvi. *WHO PAYS FOR UNIVERSAL SERVICE? WHEN TELEPHONE SUBSIDIES BECOME TRANSPARENT* at 119. The calculation involved only residential services. Had business services been included, the estimated welfare loss would have been much greater.
- xvii. The absence of a subscriber line charge would have required long-distance rates to be 2.5 cents per minute higher, or about 20.5 cents per minute. Assuming an average price elasticity of long distance service of -0.72, long distance calling minutes would have been 10 percent lower.
- xviii. *See, e.g.,* Ross Eriksson, David L. Kaserman, and John A. Mayo, *Targeted and Untargeted Subsidy Schemes: Evidence from Post-Divestiture Efforts to Promote Universal Telephone Service*, 41 J. OF L. & ECON. 477, 485-502 (1998).
- xix. Article 28, EU General Data Protection Regulation (EU) 2016/679 ("GDPR").

Notes

Notes

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

*Our associated offices

www.hoganlovells.com

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

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

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

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

© Hogan Lovells 2018. All rights reserved. 1032536_1218