International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2022

Ninth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Brave New (Virtual) World


Jenny L. Colgate


Caitlin M. Wilmot

Rothwell Figg

Introduction

Imagine that you're sitting on your sofa, scrolling through your social media feed, when you see a video posted by a friend attending a concert in another country. Within an instant, you are teleported halfway across the world, where a hologram version of yourself can experience the concert in real time. Beyond just hearing the music, you're able to feel the vibrations of the bass, get a panoramic 360-degree view of the venue, and make eye contact, sing, and dance with your friend and the other concertgoers. Head banging and heart racing, it feels as though you are part of the crowd, attending the concert in person, because despite being physically miles away, in every other sense you are there.

This is just one of the many virtual experiences envisioned by Facebook in the original presentation of its metaverse as part of its Connect 2021 event held last autumn.[1] It was at this same conference that Facebook announced its name change to "Meta", a not-so-subtle proclamation of the company's commitment to and focus on the building of futuristic technology to better connect people. Originally coined by Neal Stephenson in his 1992 science-fiction novel *Snow Crash*, the term "metaverse" has been used in connection with the idea of an all-consuming, omnipresent virtual world running in parallel to, and often intertwining with, the physical world. From an etymology standpoint, the prefix *meta-* is derived from the Greek word μετά, which encompasses a wide variety of meanings, including "after", "alongside", and "beyond" (as in metaphor, a figure of speech that extends *beyond* literal meaning) or denoting a change of place or state (as in metamorphosis). Therefore, when combined with the suffix *-verse*, we understand the term "metaverse" to mean a reality that extends beyond the confines of time and space as we know it, running alongside and transcending our existing reality.

But what exactly *is* the metaverse and what does it look like? Nobody really knows for sure yet. Just as it was hard for people to comprehend what the Internet was back in the 1980s, it is difficult to conceptualise or define the metaverse while the technology is still being developed. What we do know is that it will entail augmented, virtual and mixed reality technologies that effectively create an immersive online experience, or an "embodied Internet" where users are not just passively scrolling, but actively interacting in a fully realised computer-generated world tailored to their lifestyle.[2] According to some scholars, the metaverse will have five primary features: (1) *persistence* – the metaverse will exist regardless of time or space; (2) *synchronicity* – users will be able to interact with one another in the digital world in real time, reacting to their virtual environment just as they would in the physical world; (3) *availability* – any number of users can log on simultaneously; (4) *economy* – participants will be able to supply goods and services in exchange for value recognised by others; and (5) *interoperability* – users will be able to use digital assets across different experiences in the metaverse.[3]

This convergence of the physical and digital realms will impact all aspects of our lives, including social connections, entertainment, fitness, work, education and commerce. The metaverse will shift how we interact with technology, such that virtual objects will blend in with our physical environment and the digital world will mimic our physical life. Through the use of 3D avatars and animated holograms, users will be able to create digital meeting spaces for work, hang out with friends living across the country, play a round of tennis in their living room, travel and explore every corner of the world (and even fantasy worlds), attend classes at any university, enjoy a virtual shopping experience from your couch, and use digital assets to purchase virtual objects or exclusive experiences. Through non-fungible tokens (NFTs), or non-interchangeable cryptographic assets that live on blockchain, metaverse participants can exert their virtual spending power to buy unique digital assets, from Nike sneakers for your personal avatar to a house next to Snoop Dogg.[4] And as the scope of brain-to-machine interactions expands with the evolution of Augmented Reality (AR) headsets, Virtual Reality (VR) glasses, hand, eye and body movement sensors, as well as biometric sensors, we will be able to create a mixed physical and digital interface with contextualised artificial intelligence that responds to a head nod, a voice command, or the slightest movement of a finger.

But who will ultimately build and control the metaverse? For starters, it is worth noting that there is currently more than one metaverse. Many more, in fact. Although social giant Meta tends to dominate the buzz around the forthcoming virtual world, several other tech and software companies are building, or have already built, their own versions of the metaverse, including Epic Games, Niantic, Roblox, Nike, The Sandbox, Decentraland, and Microsoft. Yet despite the independent development efforts, many wonder if there will inevitably be one master metaverse operated by tech behemoths such as Meta, Google and Amazon. And while blockchain is promised to be an integral part of the metaverse, with a decentralised network such that users can all "build on" the technology without a central supervisory authority (as was the original intent of the World Wide Web), there are concerns about major corporations obtaining, and potentially exploiting, control of these virtual worlds.[5]

What's perhaps even more pressing than avoiding a corporatocracy is the establishment of the law of the land in the metaverse. Without a doubt, the metaverse is a new frontier, and largely uncharted territory in the legal context. As we begin shifting how we interact with technology, into an ever more digital/physical co-existence, we will need to consider how the rules and regulations of the real world apply in the virtual world, and what new laws will need to be put in place to govern our

digital interactions. For instance, would Starbucks have a claim for trademark infringement if someone sets up a virtual coffee shop in the metaverse using its famed logo, even though it is not being used in connection with "real" coffee? Can you sue someone for nuisance for building an ugly virtual house next to yours that detracts from the value of your virtual property?

More importantly, how do you prevent someone from creating an avatar that looks, sounds, and acts just like you, but isn't you? Are you able to keep your real identity wholly separate and untraceable from your virtual persona and how you portray yourself in the digital world? Can companies use your personal data collected in the metaverse for targeted advertising across both realms, or for research? And with digital assets tied to real monetary value, how do you make sure that transactions conducted in the metaverse are secure?

As the pace of technology far exceeds the speed of regulation, it is clear that there are more questions than answers when it comes to the legal framework for the metaverse. While there are many legal issues at play, concerns about privacy and data security are at the forefront of the discussion, especially as we continue to navigate and grapple with this critical area in the physical world. The importance of protecting personal data cannot be understated and before plugging into the lawless expanse of the metaverse, consumers and legal professionals alike should consider and explore exactly what and how much personal data is at stake, and the real-world risks of living in a virtual world.

Factual Background

If you thought companies harvested a lot of personal data now, just wait until the metaverse arrives. The metaverse will allow for much more intimate and expansive data collection, analysis and use than exists today. Physiological expressions (such as blood pressure, breathing rate, gastrointestinal motility, sweating), biometric data (such as facial expressions, eye movement, physical proportions, and vocal inflections), body language, and social behaviours are all among the data that will be regularly collected, stored, analysed, and used by third parties for commercial gain in the future. Our homes and surroundings will also be constantly tracked and monitored, as we are. The question remains how comfortable people will be with all this tracking and how the laws should develop to protect people from harm.

In this chapter, we consider three categories of laws: (1) privacy; (2) data security; and (3) intellectual property. Each concerns different kinds of harms and offers unique protections. Privacy law affords individuals protection of their personal information from unauthorised processing and disclosure by third parties. Are you comfortable with companies collecting, processing, analysing and using for commercial purposes increasingly intimate levels of data about you? What if they share this data with your doctor to diagnose health issues, or your insurance provider, and it drives up your insurance premiums? What if they use this data to advertise health-related products to you about conditions that you didn't even know you had? What if your boss is with you at the time that ad comes through, and questions your ability to do your job based on the condition?

Data security law protects data from unauthorised disclosure and access, which has traditionally been in the form of hacks and leaks. In more recent years, "phishing" has become increasingly common. This is where cybercriminals "pose" as someone they are not in order to persuade you to provide them with sensitive personal information, such as login credentials (so they can access even more information about you) or credit card numbers. This "posing" is often done via fake email addresses and messages that lead users to conclude they are legitimate companies with whom the user carries out business. In the metaverse, "phishing" could reach a whole new level. Instead of using email addresses and written messages, cybercriminals may use avatars that resemble legitimate individuals with whom a user does business – complete with voices, eye movement and social behaviours that mirror the "real" person. Worse yet, imagine if a cybercriminal hacked into your avatar and was able to gain access to your identity. (Picture the scene in *Harry Potter* where Harry and Ron drink Polyjuice Potion to "become" Crabbe and Goyle, the friends of Draco Malfoy (the "bad guy"), so that Malfoy would tell them trusted information.)

Finally, intellectual property law concerns the protection of rights of the creators and owners of intellectual property, including creative works, inventions and confidential information that derives economic value from the fact that it is not generally known or accessible. How does the existence of a metaverse affect these rights? How does one identify *who* an infringer is if the infringement occurs on the metaverse, in a world of avatars? And taking the earlier example of assuming another's identity, what if a competitor poses as an employee to gain access to corporate trade secrets? Or what if a disgruntled employee uses an avatar to share confidential corporate information, such that the sharing cannot be traced back to the employee? Also, what type of "intellectual property" (if any) is all of this data that companies are collecting and processing? At what point does an *individual's* personal information become *corporate* property, and if that data is processed and analysed such that it takes on a new form and gains independent value, then what is that property that results? And to whom does it belong, and how is it protected? Is it a trade secret covered by misappropriation law; is it "confidential information" protected by current unfair competition laws; or is it something new? Does a new legal regime need to be developed to protect this property?

Another question is whether this information and behaviour is even worth protecting. In this new society, more than ever before, *everything* will be data driven, and with that comes increasing risks in the form of mass surveillance, having purchase decisions controlled by corporations that arguably know you better than you know yourself, and increasingly "tunnel visioning" the ideas, information and news to which one is exposed. Is the metaverse the type of society that we want for our children? If this is not the future we want, then what can we do to change it?

Privacy and Cybersecurity Legal Considerations

Rethinking data privacy – Existing laws assume data is collected in and transferred between countries; there is a dichotomy: personal *vs.* non-personal data; and "gateways" exist between cyber spaces

Data privacy laws must change. They are wholly inadequate in view of the forthcoming metaverse in many ways, including that the laws assume that: (1) data is collected in and transferred between countries; (2) data localisation is required; (3) there is a dichotomy of data: "personal" and "non-personal"; and (4) there are "gateways" between cyber spaces, and that those gateways are text driven. All these assumptions are being tossed to the wind with the metaverse, and the privacy laws must catch up. Indeed, as we should have already learned based on the recent proliferation of data privacy laws, it is much easier to create technology around

privacy and security laws than it is to later force existing technologies into compliance with subsequently adopted laws.

First, existing data protection laws assume that data is collected in and transferred between countries. Take, for example, the General Data Protection Regulation (GDPR). Article 44 ("General principle for transfers") states:

> "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization.*"[6]

The articles that follow address, *inter alia*, transfers on the basis of an adequacy decision, transfers subject to appropriate safeguards, and derogations for specific situations. All these provisions discuss data being transferred "*to a third country or an international organization*".

What if data is transferred to the metaverse – is that a "transfer" under GDPR, even though it is not a third country or international organisation? It probably depends on what happens with the data in the metaverse. Because data transferred in the metaverse does not stay in the metaverse, and it ultimately ends up in the hands of someone that is geographically located somewhere, some will argue that the law need not change. Of course, in the metaverse, who someone actually is and where they are actually located may not be obvious. This is precisely what makes data transfers (and existing data transfer law) in the metaverse so difficult. Indeed, part of the lure of the metaverse is the idea of escaping the physical world. Yet our laws are tied to the physical world. How do users comply with laws based on the geographic location of data, in a metaverse where there is no geography? And how do countries enforce data transfer laws when transfers are happening in a metaverse among avatars?

Second, a related geography-based issue is the idea of data localisation. The aforementioned data transfer laws exist because countries want to protect the personally identifiable information of their residents. Data transfer laws allow countries to assess the protections of other countries, and if they are deemed adequate, allow transfers to those countries (via adequacy decisions). If they are not deemed adequate, then transfers may only be permitted in certain situations; for example, if the entity receiving the data agrees to treat and handle the data in an acceptable manner. In July 2020, the Court of Justice of the European Union issued its decision in a case known as *Schrems II*, wherein the Court invalidated the European Commission's adequacy decision for the EU-US Privacy Shield Framework based on the Court's disapproval of the nature of the US government's access to private sector data.[7] In other words, the Court disapproved that the United States seemingly prioritised surveillance over privacy. As a result of the sweeping language in the *Schrems II* decision, it has been unclear whether certain personal data of EU citizens can be transferred to the United States *under any circumstances*, particularly where that data may be of interest to US intelligence programmes (which especially applies to big technology companies).

In the aftermath of *Schrems II*, various data protection authorities have taken a zero-risk approach to US technology companies' processing of data from the EU. Almost any data can be contorted into "personally identifiable data" if viewed in certain ways. For example, Google Analytics' provision of analytics services based on IP addresses has recently been under a microscope, and France and Austria's European data protection authorities have declared websites' use of these services (whose servers are in the United States) to be in violation of the GDPR.[8] Thus, the push for "data localization" is clear. Companies like Google and Meta can store and process data in the EU, or their services can be off-limits to EU citizens. Indeed, in February 2022, Meta announced in its annual report that it was considering shutting down Facebook and Instagram in Europe if it can't keep transferring data back to the United States.[9]

In view of these recent events, one can't help but wonder how data localisation in the context of the metaverse can possibly work. If there is to be a universal metaverse (or metaverses), where people from all over the world can "log in" and interact, then strict data localisation requirements seem impossible. Big technology will not be able to decipher who is from where, what laws apply, and process and store that data only in certain geographic locations. Also, for the interoperability of the metaverse to work as it has been envisioned, it seems necessary that data be transferred freely, unhindered by the concept of different laws applying to different companies and different users. Or, in view of the recent decisions coming out of the EU, are we to believe that the EU will insist upon geographically distinct metaverses – for example, an EU metaverse that is unique from a US metaverse?

Third, many existing privacy laws assume that data categorisation is strictly binary – "personal" or "non-personal". But some data is not so clearly delineated. For example, consider the IP address data that is at issue in the Google Analytics cases. By itself, this data is not personally identifying; however, once linked with data concerning a user's web browsing behaviour, it becomes personally identifying. Still, the information does not necessarily reveal your true identity. Unlike your face which you only get one of, and once stolen you are damaged forever, the same is not true about an IP address and browsing history. This "third bucket" of data will likely grow in size in the coming years, thanks to the metaverse. Remember that a basic principle of the metaverse is that people interact through avatars. Those avatars are, in some ways, like upgraded versions of IP addresses, in that they will be used to link together data about one's behaviour in the metaverse. However, unlike IP addresses, they will also be collecting personal data directly from a user's own body and surroundings at the same time. That additional information has different levels of sensitivity. For example, connecting one's avatar to their metaverse activity and heartrate is probably not very different from Google Analytics' current process of mining data linked with one's IP address. However, if you add in highly sensitive personal data (e.g., iris scans and genetic information), then obviously the calculus of how to treat this information is very different. Thus, the issues that data protection officers have been tackling over the last couple of years concerning IP addresses (and coming out on both sides of the fence) will continue to evolve, as technology develops.

Fourth, a major difference between the Internet and World Wide Web as we know it, and the idea of the metaverse that lies ahead in our future, is the seamlessness of the environment. Those "seams" are important to how current data privacy laws work. Think, for example, of cookie consents. Per the EU e-Privacy Directive, each time someone visits a website that is hosted in the EU, owned by an EU company, or caters to EU citizens, the website must inform them that cookie technologies are being employed, and users are given an option to refuse to allow cookies.[10] How will this requirement work when there are no longer "websites" and the people can just "walk" from one cyber space to another with their avatar? Similarly,

is there a place for privacy policies? The envisioned metaverse is very graphic in nature. How would text-driven policies and consents be received in this new environment? Think of yourself walking through an outdoor mall today, and every 20 feet when you come upon a new store someone stops you and asks you to consent to the store's privacy and tracking policies. It would undoubtedly be annoying and distracting. At the same time, imagine yourself walking through an outdoor mall today, but in order to shop there you have to put on a full-body suit and headgear that enables all the companies in the mall (and others) to analyse everything about you – your eye movements, your thoughts, your heart rate, your breathing, your sweating and more. It would likely be invasive to the point that you would consider shopping elsewhere.

Even more critical is how consent mechanisms will be employed where children are concerned. Most countries have laws that provide for the special protection of children's personal data through age verification techniques and mandatory parental consent for certain uses of children's personal information. In the marketing and data-driven metaverse, administrators will need to prioritise implementing measures to deter children from providing their personal data and enforcing age restrictions to protect children from predators.

These are just some of the privacy-related legal considerations that law and policymakers, as well as technologists, must think about in the coming years.

Rethinking data security – what are reasonable safeguards, how should data breach notification work, and can data breaches be rectified?

With workplace and social engagements moving to the digital world, as well as a metaverse e-commerce market projected to reach well over $500 billion by the year 2030, users will significantly increase their digital footprint in the metaverse, injecting unprecedented volumes of personal data into cyberspace. Naturally, however, more data attracts more hackers and bad actors, and the risk of theft of sensitive or confidential data will be a paramount concern. Furthermore, the valuable capabilities of connected devices around our homes and offices used to monitor our behaviour and actions in real-time, will increasingly make these devices prone to cyberattacks.

In addition to hacking concerns, the metaverse will also bring about increased security risks in the form of data breaches. Current data security regulations suggest that data controllers should employ reasonable technical, administrative and physical security measures to protect consumer data. But will "reasonable" measures be sufficient to protect against data breaches in the age of the metaverse? For example, how will employees verify that their metaverse work environments are secure and their co-workers' avatars are legitimate? How will companies police their employees on the metaverse, when only a couple of years ago many companies did not even trust their employees enough to allow them to work remotely?

Data security measures in the metaverse may also look different due to the prevalence of blockchain-based transactions. For example, the GDPR provides for "data controllers" who determine the purpose for which data is processed and the way data is processed, and "data processors" who process the data on behalf of the controller. Under a decentralised blockchain network, which gives users more control and power over their personal data, the data controller could be the user. While empowering, the lack of a centralised authority and putting the trust in individual consumers to self-safeguard could prove disastrous, such as last year, when software developer and crypto-enthusiast Stefan Thomas transferred around $250 million worth of Bitcoin into a digital wallet, and then lost the password (and thus access) to his mega-millions.[11] On the other hand, the idea of handing over access and control of personal data to metaverse administrators, collecting and processing massive amounts of big data tied to the intimate details of our everyday lives (for marketing, research or other purposes) could also lead to bad outcomes.

"Reasonable" physical security requirements would likely be very similar to those already in place at data centres; however, technical safeguards may be different. For technical security to succeed in the metaverse, measures like passwords, encryption and authentication, and the policies and procedures surrounding access to various parts of the metaverse, will have to be implemented in a way that is robust, but without negatively impacting user convenience. As with the cookie consents described above, no user wants to be inundated with gateway checkpoints as he or she navigates through the metaverse, even though this may conflict with the fundamental data protection principle of transparency. This is another area where blockchain technology may come into play, as a technical solution capable of providing transparency, validation and interoperability.

The application of data breach notification laws in the metaverse presents another unique set of challenges. For instance, state data breach notification laws typically require a company to notify a user affected by a data breach (usually within 30 to 60 days of the incident) that a breach has occurred and to identify the specific steps the company is taking to remedy the breach. However, the immutability of blockchain technology begs the question of how certain data breaches in the metaverse could ever be rectified once leaked. Furthermore, would sending a notification of a breach in the metaverse through the metaverse itself be sufficient to constitute the required notice? And will it even be possible to notify users in the real world of a breach of their personal data in the metaverse without compromising their right to privacy?

As the security of personal and confidential information in the metaverse is paramount to its success, these are more legal issues that will need to be tackled from the outset and implemented by design, rather than retroactively after problems arise.

Rethinking intellectual property – heightened risks of misappropriation of trade secrets and confidential information, and is there a new intellectual property right that needs to be protected with a new legal regime?

There are also numerous intellectual property concerns that come into play with life in the metaverse. At the forefront is the heightened risk of misappropriation of trade secrets and the disclosure or misuse of confidential information.

For instance, imagine talking to your boss via the metaverse one day about business plans for your company's top trade secrets, only to learn the next day that your boss was not there, and someone else had hacked her avatar. How would you identify the imposter? Will the metaverse also make it easier for rogue employees to flout company rules, and potentially disseminate corporate confidential information, without being caught? As users may choose to adopt a virtual persona or multiple virtual personas (e.g., via the user's selection of a human or non-human avatar, gender, different "physical" characteristics, voice, gestures, clothing, etc.), which may be wholly divorced from the user's identity and likeness in the real world, it can be extremely difficult to truly know who is who in the metaverse, and to locate the real-world individual or entity who may have improperly acquired your intellectual property rights.

In some ways, this problem is not unique to the metaverse. Similar concerns were raised in the early days of the Internet. However, the metaverse is distinct from the Internet in that it lacks a "paper trail" of communications. While blockchain technology may provide for the validation and documentation of transactional data, there may be no such recordation of other interactions in the metaverse, such as the exchanges between avatars in a meeting space, messages shared in a game, or speaking through headsets. As these types of actions are difficult to document, it remains unclear how one could trace an improper disclosure or misappropriation of confidential information back to a specific individual or entity. Due to this gap in accountability and consequences, it is expected that there will be a heightened risk of misappropriation of these types of intellectual property in the metaverse, at least initially. Even more concerning is if the metaverse service providers were to actually record and mine these personal interactions for their predictive advertising algorithms or a similar monetisation. Such recordation could effectively eliminate privacy as we know it.

Based on the unique nature of the metaverse, and the collection and processing of colossal amounts of personal data, it is also unclear at exactly what point an individual's personal information may become corporate property, and what other types of "intellectual property" may result from any transformation of that property into something of value. It is very possible, if not likely, that new forms of intangible creations of the human intellect will be developed through the metaverse, and we may well have the exciting opportunity to explore new legal rights under a future-focused regime.

Conclusion

The metaverse is a brave new (virtual) world. We would all be well served by technologists and lawmakers from all over the world coming together to discuss how they envision the future – technologically speaking and legally speaking – and collaboratively designing this future in a way that maximises its potential and minimises its risks.

Endnotes

1. The Metaverse and How We'll Build It Together – Connect 2021, Meta (October 28, 2021), available at https://www.youtube.com/watch?v=Uvufun6xer8&t=775s.
2. Newton, Casey, *Mark in the Metaverse: Facebook's CEO on why the social network is becoming 'a metaverse company'*, The Verge (July 22, 2021), available at https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.
3. Norton Rose Fulbright, *The Metaverse: The evolution of a universal digital platform* (July 2021), available at https://www.nortonrosefulbright.com/en-us/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform.
4. *Nike Creates NIKELAND on Roblox*, Nike News (November 18, 2021), available at https://news.nike.com/news/five-things-to-know-roblox; Hissong, Samantha, *Someone Spent $450,000 for 'Land' Next to Snoop Dogg's NFT House*, Rolling Stone (December 7, 2021), available at https://www.rollingstone.com/culture/culture-news/sandbox-decentraland-virtual-land-sales-soar-metaverse-nfts-1267740/.
5. Brooker, Katrina, *'I Was Devastated': Tim Berners-Lee, The Man Who Created The World Wide Web, Has Some Regrets*, Vanity Fair (July 1, 2018), available at https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets.
6. General Data Protection Regulation (GDPR), European Parliament and the Council of the European Union (2018), available at https://gdpr-info.eu/.
7. Judgment of the Court (Grand Chamber), Court of Justice of the European Union (July 16, 2020), available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9710189.
8. *See, e.g.*, Colgate, Jenny, *Can European Websites use Google Analytics and Similar Services Without Violating the GDPR?*, Rothwell Figg's Privacy Zone (January 19, 2022), available at https://www.theprivacylaw.com/2022/01/can-european-websites-use-google-analytics-and-similar-services-without-violating-the-gdpr/ (Austria); Bryant, Jennifer, *CNIL is latest authority to rule Google Analytics violates GDPR*, IAPP (February 10, 2022), available at https://iapp.org/news/a/cnil-is-latest-authority-to-rule-google-analytics-violates-gdpr/ (France).
9. SEC Form 10-K (for the fiscal year ended December 31, 2021), Meta Platforms, Inc., available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf.
10. E-Privacy Directive, European Parliament and the Council of the European Union (2002, amended 2009), available at https://edps.europa.eu/sites/default/files/publication/dir_2009_136_en.pdf.
11. Popper, Nathaniel, *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes*, The New York Times (January 12, 2021), available at https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html.

Jenny L. Colgate is a partner who is an experienced litigator, a creative strategist, a trusted advisor, and a thought leader. Her practice is largely focused on litigation for a clientele that includes manufacturing, technology, and publishing companies. Jenny also consults with clients regularly on IP strategy, contracts and licensing negotiations, privacy, and defamation/libel reviews.

Jenny's litigation experience extends into all facets of intellectual property and technology-related tort and contract matters, including patents, trade secret, unfair competition, trademark, copyright, breach of contract, and fraud-related claims. She is also a frequent speaker on privacy issues in the workplace and in healthcare.

She received both a J.D. (*magna cum laude*) and LL.M. (*magna cum laude*) in Intellectual Property from the University of New Hampshire Franklin Pierce School of Law. She previously received a B.A. from the University of Pennsylvania (*summa cum laude*).

Rothwell Figg
607 14th Street, N.W., Suite 800
Washington, D.C., 20005
USA

Tel: +1 202 783 6040
Email: jcolgate@rfem.com
URL: www.rothwellfigg.com

Caitlin M. Wilmot focuses her practice on patent litigation, post-grant proceedings before the Patent Trial and Appeal Board (PTAB), patent prosecution, opinions, counselling, and privacy. Her experience covers a broad range of technologies, including chemical, pharmaceutical, electrical, and mechanical. Caitlin helps clients anticipate, and prepare for, all the challenges that may come their way: pitching an invention to potential investors; maintaining a competitive edge through IP enforcement; selling or licensing technology; or conducting due diligence in bringing a product to market.

Her work covers the full spectrum of IP representation for her clients. A partial list would include drafting and prosecuting patent applications, filing trademark applications and copyright registrations, consulting on building a robust IP portfolio, advising on IP enforcement, contract review, and all aspects of litigation, including drafting substantive pleadings and motions, preparing expert reports and inventor declarations, and assisting with high-level strategy development.

Rothwell Figg
607 14th Street, N.W., Suite 800
Washington, D.C., 20005
USA

Tel: +1 202 783 6040
Email: cwilmot@rfem.com
URL: www.rothwellfigg.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group