

Digital Trust

Creating trust in a digital world

Hogan
Lovells



DIGITAL TRANSFORMATION

Introduction

We know that digital trust is critical to digital adoption and there is strong evidence that businesses capable of establishing trust in their digital products, services and overall digitized delivery will grow considerably more than those who do not. This applies across the spectrum and in core sectors that our clients operate in, such as financial services, transport and healthcare which are digitizing rapidly. It is key.

Law is central to establishing trust in digital products and services because certainty on matters such as legal interpretation, regulatory applicability and enforceability of rights vis a vis digitized as opposed to traditional interactions, can make or break trust in what is being offered. If a consumer cannot be sure that they have “exclusive property” in their assets, or that they will benefit from legal redress in the event that technology-based services sold to them do not deliver, they will not be confident to interact or scale their interactions with these offerings. There is also a significant issue that failure of digital trust in respect of one product, service or interaction can quickly spread to create lack of confidence in all such digitized business offerings in a particular area (or even worse, a crisis of confidence in digital interactions broadly). So it is important to get legal certainty right from the beginning.

In preparing this paper, we asked ourselves how can we be proactive in supporting building a trustworthy digital world? How can we ensure that when clients and consumers are faced with reasons to question digitized products and services and new technologies, we have built a solid foundation on which to withstand the ebbs and flows of digital adoption? This whitepaper contains 12 chapters, each reviewing a key sector or theme in the context of digitization. We have sought to identify the main legal certainty and trust markers that apply to each, and have provided quick reference, easy to apply recommendations to improve performance on these factors going forward, all with a view to enhancing digital trust.

These topics are significantly interconnected by nature – just as trust failures can easily spread into lack of confidence in digital adoption broadly, we consider that trust establishment is also strongly interconnected and infectious. We believe that businesses and lawyers need to move forward on this together across sectors, specialisms and market segments. We have brought together the multiple chapters on this topic in one place all united under the umbrella theme of Building Better Digital Trust.

Contents





Digital Identity

Digital identity is key to building trustworthy interactions in digital activities and yet, itself, has struggled to win widespread trust. In this chapter, we explore how safe and secure actions, interactions and transactions using digital identity are, and what can be done to improve this.

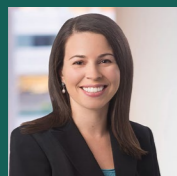
Authors



Elizabeth Boison
Partner
Washington, D.C.



Leopold von Gerlach
Partner
Hamburg



Sara C. Lenet
Partner
Washington, D.C.



Bryony Widdup
Partner
London



Luke Grubb
Consultant
London

Introduction

Determining an individual’s identity is critical to most of daily life, and this is no less true of our online activities. As our lives increasingly move online, fraud and other criminal activities become more and more sophisticated. Alongside this, our personal data is recorded and stored in ways that mean that the individual is rarely in control of their own information. Securely authenticating the individual is necessary to protect their data, assets, and privacy. By allowing us to identify the actor in online activities, and giving individuals control over their own data, digital identity (“dID”) is the key to digital trust.

Analysis: Digital Identity – safety and security in actions, interactions and transactions

While there are solutions beyond dID that are in development to address issues such as online fraud, certain efficiencies offered by emerging technology are impossible to bring to fruition without digitalized processes for identification.

Take RegTech and digital anti-money laundering capabilities: while the technology exists to trace the movement of digital assets through online and on chain transactions, these solutions can only go as far as the analogue world will allow them if there is no digital solution to identifying the sender and benefactor of relevant assets.

There are platforms aiming to digitalize the process of verifying an identity, but at present these do not take a holistic approach to identification. A dID that could be plugged into a trading platform using, for example, a digital wallet could simultaneously hold data that could be used in health care, insurance, education and job applications, or in engagement with councils and other public offices. A sophisticated dID could bring together all information to become a one-stop shop for the user.

On the other hand, having all such identification information held centrally by either a public institution or even a large private tech firm gives rise to concerns as to protection of privacy and over-concentration of power. In light of this, decentralized solutions may offer more comfort for individuals and also provide users with greater control over their own data.

As well as safely authenticating who is carrying out a transaction, new dID solutions are being built that allow the user to protect their privacy by giving them discretion as to who sees what, and when. Examples include Zero Knowledge Proof (“ZKP”), which uses encryption to provide proof that data is correct without revealing further information. This is of particular use when there is a lack of trust from both parties: person 1 does not want to interact with an anonymous user, but person 2 does not trust that person 1 will not store their identification data for other uses. If used correctly, ZKP can

simultaneously build privacy into the internet while stopping bad actors from remaining fully anonymous.

So, what has held dID back? Legal uncertainty and lack of consistency across solutions provided today leave users, both in Business-to-Business (“B2B”) and Business-to-Consumer (“B2C”) scenarios, unable to trust in the solutions available. As a result, dID is therefore both the chicken and the egg to digital trust; we simultaneously need it to trust digital activities, but struggle to trust in it in the first place.

ID cards in themselves can be a polarizing topic, even in the analogue world. Knowing this, policymakers may hesitate to prioritize policy in this report or direct the market towards one or more types of solutions or providers for fear of creating unnecessary tension.

Where legislators have started the drive towards dID, such as in the European Union, complex issues including security standards, the parameters of its functions, and data standards have been cause for long debate. Security standards are clearly crucial to maintaining public trust, given the threat of identity theft or cyberattacks and the inherent tensions with privacy continue to make this a very difficult area.

Leveraging blockchain to address concerns may also challenge existing legislative principles. General Data Protection Regulation (“GDPR”),

for example, includes the right to be forgotten, and many blockchains are built specifically to be immutable. So relevant personal data seemingly cannot be held in blockchain-based databases, although on the other hand they may offer helpful decentralized solutions. But such decentralized solutions may also themselves go too far for comfort. Self-sovereign identity via self-custodied wallets may appease those who are skeptical of a centralized authority holding their data, but this opens the same debate as in the digital asset space, where there are concerns over how well individuals can be trusted to safely store their private keys. Transferring the risk of identity fraud from faking documents in the analogue world, to stealing or scamming people into releasing their private keys in a digital one, is no solution at all.

Not only will legislators need to decide on these standards domestically, they will also need to consider dID's interoperability across jurisdictions. Internationally accepted data standards will be needed, which will be far more complex than existing standards to analogue passports.

Given the complexity of these debates and decisions, it is likely to take some time before a holistic solution is available. To some degree, given the policy concerns with imposing centralized dID, it is being left up to the market to create alignment and interoperability. However, all too frequently at present, market participants default to analogue solutions in order to come to trusted outcomes which can severely limit functionality. On the other hand, education remains a challenge for some citizens who are still struggling with well-established technology like contactless payments. As such, there is a great need for simple solutions that negate the danger of citizens being excluded from participation (and similarly, overcomplexity might actually encourage misuse and fraud) which will also delay bringing forth dID's essential contribution to digital trust.

Key recommendations

1 Follow the 3 Cs

Consistency, compliance and communication. Solution providers need to seek high quality legal and compliance advice on toeing the line carefully to retain the trust of its audience.

2 Due diligence

Conduct appropriate due diligence on platforms used by your own business and that of counter parties in B2B settings. Consider matters such as legal and cyber security robustness, as well as user-friendliness and interoperability.

3 Legal clarity and future-proofing

In the absence of clear policy direction and an ever-evolving legal environment as to all matters digital, firms will need to ensure they are aligning to anticipated future required standards so that the arrival of legislation does not trigger an overhaul of plans.





Digital Property

The digital world opens up many possibilities for owning and exchanging digital property. In order to fully embrace a digital life, regulation, that enhances digital trust, is essential. In this chapter, we examine how we can securely own property in a digital life.

Authors



Jennifer Dickey
Partner
London



Olaf Gärtner
Partner
Munich



Joel Smith
Partner
London



Martin Strauch
Counsel
Munich



Lavan Thasarathakumar
Senior Advisor
London



Introduction

Whether it is purchasing a NFT, entering the metaverse, or buying products through online gaming sites, our digital lives are becoming increasingly complex. As these new opportunities to embrace a digital life emerge, we need trust in the law around digital property, which is essential to ensuring consumers can buy, protect and enforce their rights in a digital world.

As we examine below, courts, the world over, have readily risen to the challenge of applying existing remedies to enforce and protect rights in digital assets and to navigating questions of jurisdiction, but there remain some legal and policy gaps, which might helpfully be filled in the near future, to both support and encourage trustworthy digital adoption.

Analysis: How can we own property securely in a digital life?

Digital ownership (NFTs/virtual assets in the metaverse/elsewhere)

Taking a non-fungible token (“NFT”) as a core example, it is a digital unit of data built on a digital ledger, a blockchain. It is minted, powered by a smart contract. As a unique token, it is transparent and traceable, providing proof of ownership or a certificate of authenticity either to an associated purely digital asset (such

as digital art or a limited edition skin for an avatar for gaming), to a physical asset (such as access to a rare collector’s bottle of spirits or to a limited edition fashion garment) or to an experience (exclusive access to backstage at a concert). It may be redeemed in exchange for the physical asset or traded as a commodity with the corresponding rights to the underlying asset. Unlike traditional forms of title to property, the NFT provides an immutable ledger of ownership. It may also be used to detect or prevent counterfeiting of genuine, branded products (whether trainers or medicines). NFTs play an important part in the numerous metaverses in providing reassurance to consumers who wish to purchase digital assets as a verifiable certificate of title.

Looking forwards, we see developments in the regulation of crypto assets, that aim to ensure a level playing field for consumers and investors alike, will help in building trust. We see scope to help ensure that the terms of each smart contract associated with digital assets, such as NFTs, are set out in a clear and understandable way, to avoid misunderstandings about the nature and exclusivity of the rights attached to the digital asset (for instance, in digital artwork scenarios, the right to enjoy and use the attached work and whether there are limitations through copyright or whether sale of the NFT is subject to paying any royalty-share or claw back in favor of the original owner for uplifts in value).

Methods of enforcement in relation to digital assets

All over the world, courts have quickly risen to the challenge of applying existing remedies to enforce and protect rights in digital assets and to navigate questions of jurisdiction. However, the technicalities of enforcement and details of how digital assets that have been misappropriated can be seized, differ from country to country. Given that digital asset networks are frequently entirely international and boundary-less, this means enforcement and recovery remains inherently complex.

In general, courts and due process have had to adapt in all stages of a matter. We have seen adaptation in enabling service of process in novel ways, new thinking in pre-judgment protection, including duties or orders to disclose information about digital assets, and interim protective measures during proceedings, such as freezing orders. Once a party has obtained judgment, enforcement in relation to a digital asset will depend upon the precise structure and technicalities of the asset. In most jurisdictions there are already ways to seize or transfer, by way of force, physical hardware devices, software, but also specific digital assets. This includes ways to obtain respective passwords and private keys from debtors, e.g. by threatening fines or even prison.

The law quickly adapts to new phenomena, such as blockchain and digital assets and continues to evolve with new technology. Companies and individuals dealing with or investing in these assets can therefore be confident that courts and the rule of law will adapt with changing technology to continue to protect property rights. It remains to be seen whether lawmakers deem it necessary to provide special rules for digital or crypto-assets. Despite lively discussions, Germany, has not deemed it necessary to adapt its Civil Code so far. However, in the UK there have been several consultations in this area, along with a recommendation to introduce a new category of property into the law.

As we have already seen, certainty of ownership rights with respect to the digital property we rightfully possess is one of the most important aspects of digital trust. As digitization advances, individuals and businesses will seek increasingly to own natively digital property and real world assets, via digital means. To avoid the descent of digital systems into lawless chaos, we must have confident property ownership structures, the ability to effectively acquire and dispose of property and to enforce against those who may seek to dispossess others of their property unlawfully, to recover lost property and to receive financial compensation, where it cannot be fully returned. To date, there has surprisingly been little policy development from a property law perspective. The most notable development is that of the Law Commission of England and Wales (“The Law Commission”) earlier this year.

In light of the central importance of property rights to trust in digital assets, it is helpful that the common law courts have already started to recognize digital assets as personal property and have made a number of decisions to protect property holders’ rights within existing definitions and legal frameworks, as noted above. However, noting the increasing importance of digital assets to society, the Law Commission made recommendations to reform the legal status of digital assets.

The law of England and Wales currently recognizes something as personal property, if it is a chose in action or if it is a chose in possession; however, the Law Commission has proposed to

create a new, third category of data objects to cover digital property, the definition of which will be developed by the courts. The recommendation was made noting that this new category would cement the current common law position and provide clarity. It also harnesses the flexibility of the common law in permitting the courts to define it. However, there remain questions about how to develop trust and legal certainty in an entirely new category of property, and noting the technical nature of this, it is important that courts are well supported and equipped with tools to help them in getting this right.

Therefore it is also recommended that a technical panel be created which is tasked with creating non-binding guidance on the definition. The DIFC took an alternative approach to this, opting for a specialist court to be put in place. This is also an option; however, it could be quite costly to have a separate court and requiring applicants to make separate applications. In contrast, a technical guidance panel could slot into the current system.

Whilst not yet in force, the reforms proposed by the Law Commission are likely to set the standard for how other jurisdictions will proceed. Whilst the recommendations are made based on the law of England and Wales, its principles are likely to have a global effect given the large number of commercial contracts governed by the law of England and Wales and jurisdictions which have the Supreme Court of England and Wales as their highest court of appeal. Nonetheless, given the global nature of this technology, it is imperative that jurisdictions do not operate in silos and there is legal certainty and clarity as to the legal status of digital assets across the board; only then can boundary-less trust be developed. As such, we would endorse other common law jurisdictions to consider taking a similar approach.

Additional source:

- [Cryptocurrency disputes: five things every litigant should know – Hogan Lovells Engage](#)

Key recommendations

- 1 Understand the need for effective interaction between natural language and code, including ensuring that the terms of a smart contract are described, summarized or otherwise set out in a clear and understandable way, to avoid any misunderstandings about the nature and exclusivity of the rights attached to a relevant digital asset.
- 2 Look to existing protections and extend to virtual assets – we predict that the courts will readily apply existing principles to grant interim injunctions against owners of digital assets including NFTs or users of metaverses, where there is an infringement of a third party’s intellectual property rights. Similarly, courts will use their inherent jurisdiction or specific statutory authority to grant blocking orders against digital platform providers in appropriate cases, to force the provider to block, remove or disable access to digital assets or services, where the provider has knowledge that the owner or user of the digital asset is infringing another’s intellectual property rights or committing a criminal offence (including concerning online safety).
- 3 Companies and individuals dealing with or investing in digital assets can rely on courts and the rule of law to be protected regarding their crypto assets, but will need to understand some of the novel adaptations to process and the ways in which precedents are being defined. It remains to be seen whether lawmakers deem it necessary to provide special rules for digital or crypto-assets and so keeping on top of conversations and debates in that respect is also essential.



We also further consider digital property in the context of digital gaming in [chapter 8](#) below.



Digital Custody

As increasing levels of capital flow into digital assets globally, digital custody services have never been more essential or relevant. Understanding the risks and possible mitigations is important for institutions seeking to enter the digital asset space and to ensure there is trust in the custody solution selected for each project.

Authors



Elizabeth Boison
Partner
Washington, D.C.



Andrew McGinty
Partner
Hong Kong



John Salmon
Partner
London



Jochen Seitz
Partner
Frankfurt



Michael Thomas
Partner
London



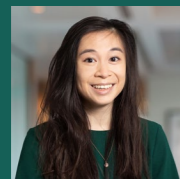
Bryony Widdup
Partner
London



Lavan Thasarathakumar
Senior Advisor
London



James Sharp
Associate
London



Christina Wu
Associate
London

Introduction

With increasing levels of capital continuing to flow into digital assets globally, an ever-growing pool of asset holders, and even governments exploring their own digital asset projects, the need to examine custody services in the digital assets industry has never been more essential and relevant. New exciting projects are being piloted and implemented so that increasingly, institutions – once reserved and hesitant – are dipping their toes into this exciting world. With new projects, come new challenges, but we often find that it is the fundamentals of storing, safeguarding and administering digital assets that pose the biggest stumbling block for making progress.

Ownership of a digital asset relies upon cryptographic techniques, and is typically (though not always) reliant upon an underlying infrastructure known as DLT.

When we refer to digital assets, we are essentially referring to intangible data that are reflected on a DLT system, in an encrypted form, the ownership of which is demonstrated by, and transferred through, the deployment of the private keys that provide for control and are used to authenticate transactions in the DLT system. Digital asset custody therefore refers to the custody or storage of the private key or keys associated with the public addresses where the clients digital assets are recorded and the ability to control operation of the client's wallet by posting transactions to the distributed ledger, all in accordance with instructions provided by the client.

This is not an asset class that traditional custodians are used to safeguarding or administering for clients. Both what is being protected and the participants involved are different in the digital space. Where traditional custodians offered connections to various stakeholders within the traditional financial markets, digital asset markets involve a range of different stakeholders and institutions which are connected in a different way.

Understanding all of the risks and possible mitigations is important for institutions seeking to enter the digital asset space and to ensure that trust is fostered and maintained in the custody solution selected for each project.

Analysis: What are the key risks associated with digital asset custody, and how can these be mitigated in order to ensure there is trust in a digital asset custody solution?

Operational approach to custody and resilience

Key to ensuring trust is knowing that the custodian offers a resilient service – in other words, it is able to protect client assets in the event of a disaster or other unforeseen event.

 [Read more in our Digital Asset Custody Paper](#)

Risks can be mitigated by implementing certain operational measures. For example, if the custodian has segregated the assets of each client, then this presents a higher level of protection for clients (even if it may result in certain operational inefficiencies in relation to the ability of the custodian to execute a client's orders). In contrast, certain custodians may employ an omnibus model which offers operational efficiencies but may increase the risk for clients of either a security breach or custodian failure or insolvency. Customers will need to be able to assess the details of a structure, which may sometimes be difficult to discern without additional due diligence, and then weigh any potential risks against the commercial benefits.

For institutions that are evaluating digital asset custodians, existing principles relating to the evaluation of critical outsourced service providers may prove to be a useful tool.

Robustness can also be significantly enhanced by the implementation of appropriate security measures in the event of an incident and business contingency planning such as developing a methodology and/or to ensure there is sufficient technical expertise at hand (whether internally or externally) to recover/replace/restore private keys in the event of a disaster.

Security Risk

Cyber security risk is fundamentally interlinked with weakness of trust in the provision of digital asset custody services – digital asset custodians have been subject to a spate of recent hacks, which in many cases have resulted in the looting of customers' digital asset wallets which has clearly negatively impacted trust. Cybersecurity risk is not a new concept, but the manner in which hackers are able to access and misappropriate assets and funds has evolved alongside the technology itself.

In these cases as things currently stand, customers are reliant on the terms presented by the digital asset custodian, and to some extent the custodian's goodwill to make whole stolen assets. Importantly (and in general terms), there is no regulatory obligation upon the custodian to make whole the customer in this scenario.

While there may be some pre-existing legal principles that seek to assign responsibility and

liability which apply in certain jurisdictions in such scenario, those principles may not neatly apply in the digital asset context. Over US \$6.2 billion worth of digital assets were lost to hackers and scammers in digital asset-related scams in 2021, demonstrating the extent of this issue.

It is therefore essential, in order to develop trust in a digital asset custody solution, to implement and maintain robust security measures that are fit for purpose (i.e. noting the significance of private keys in digital asset custody versus traditional forms of custody). A key consideration in this respect relates to the custodian's approach to hot and cold wallet storage, and other applicable security mechanisms (such as sharding or multi-signature wallets). Customers need to understand what steps the custodian has implemented to ensure that the ratio of hot-to-cold digital asset storage is appropriate given that cold wallet storage will offer stronger security resilience but less functionality and these features need to be balanced.

Client protection on insolvency

Client protections in relation to private key storage are not currently commonplace. Nor are digital assets or private keys recognized for special treatment in custodian insolvency.

This contrasts with other forms of asset that clients may be used to dealing with. One example would be "e-money" in the EU and UK, which benefits from a Special Administration regime for payments and e-money firms, designed to facilitate return of customer funds as soon as reasonably practicable.

Broadly, such protections are not available in relation to digital assets that are not regulated as regulated instruments (for example, as e-money is regulated in the EU and UK).

Given that custodian policies regarding segregation differ, and there is no specific regulatory regime providing for protection of customer assets in a digital assets custodian insolvency scenario, there is a risk of the relevant client ranking with unsecured general creditors in the event of insolvency of the third party custodian. This means that the client sits much lower in the pecking order when the insolvent party's assets are distributed to its creditors. As

a result, the client is less likely to receive the full amount of its digital assets upon the insolvency of the digital asset custodian.

Effective segregation can offer some protection in this regard – where assets have been transferred to a third party custodian's wallet on the basis of

outright title transfer to that custodian, customers should seek to ensure that appropriate contractual terms are in place to govern that relationship to ensure that the client's interests are protected and that the assets are properly segregated from the custodian's own assets (e.g. via a trust arrangement).


Key recommendations

1 Custody is a key building block for any digital asset and tokenization project, but if approached in the wrong way (without the correct questions being asked) these projects may never get off the ground, or could lead to real issues and challenges down the road.

2 For entities seeking to appoint a custodian for digital assets, we would advise particular focus on the following aspects in order to engender trust in the custody solution:

- (a) assessing the legal structure of the applicable custody arrangement, to ensure this is appropriate for an institution's requirements (and includes appropriate customer protections in the event of insolvency);
- (b) digging into the custodian's operational processes, including its approach to ensuring that it offers a resilient service;
- (c) considering the security mechanisms that the custodian implements to ensure that its clients cryptoassets are not unnecessarily at risk; and
- (d) scrutinizing the approach to regulatory compliance that the custodian is implementing.

3 There is a need for regulators/policy makers to continue to develop greater clarity as to the regulatory characterization of digital assets, the precise nature of legal property rights associated with the asset class and clarity on the approach to regulation of the services relating to digital assets, including custody.

 We also further consider digital assets property rights in [Chapter 2](#).



Digital Payments

The evolution of payments from coins to electronic bookkeeping, to arguably the next stage: tokenization, DLT and programmability, shows no signs of slowing. In this chapter, we analyze the journey to implementation of large scale digital payments solutions and how digital trust sits at the heart of adoption.

Authors



Leopold von Gerlach
Partner
Hamburg



John Salmon
Partner
London



Roger Tym
Partner
London



Bryony Widdup
Partner
London



Lavan Thasarathakumar
Senior Advisor
London



Christina Wu
Associate
London

Introduction

In recent years, powered by rapid technological advancements and fueled by the Covid-19 pandemic, the use of online payments continues to grow while the use of physical cash is on the decline. Moreover, from the first use of metal coins thousands of years ago, to the dematerialization of money and electronic bookkeeping, the advent of new technologies (e.g. programmability, tokenization, DLT) arguably represents the next stage in the evolution of money and the payments system.

A number of solutions are appearing and developing as potential candidates for alternative forms of money. Cryptocurrencies without linkages to fiat currencies or to other benchmarks such as commodity prices gained recognition for their ability to permit private and trust-less transactions, but have so far proved to be too volatile in value to be relied upon as a realistic alternative to money as a means of exchange; privately-issued stablecoins, while designed to maintain a stable value, have not yet gained the same level of trust compared to central bank money to garner mainstream acceptance.

Nevertheless, innovations in digital payments (whether in the form of stablecoins, central bank digital currencies (CBDCs) or other forms, such as programmable money) present numerous opportunities for improvements to existing systems.

Digital money certainly has some advantages:

- (1) decentralized and direct ownership models offer protection against traditional institutional failures, including insolvency (as we saw during recent banking collapses, digital money can offer risk mitigating benefits in certain circumstances);
- (2) fully fluid in ecommerce (as opposed to cash);
- (3) instant, automatic and convertible-free payment for any type of asset (including crypto) (as opposed to e-money); and
- (4) programmable and smart contract suitable (as opposed to all other forms of money) – programmability (e.g. automatic payments subject to pre-determined conditions) can provide enhancements, including simplifying user experience, reducing human error and counterparty risk, enabling micro-payments, providing for greater transparency, reduced intermediaries (and associated fees).

At the heart of the journey to the largescale adoption of any digital payments solution is to develop the public's trust and confidence in such a solution.

“
At the heart of the journey to the large scale adoption of any digital payments solution is to develop the public's trust and confidence in such a solution.
”

Analysis: What will it take for digital payments/stablecoins/CBDCs to become a better alternative to existing systems? When will be their break-through moment?

A. Privacy

One of the key benefits presented by digital payments, particularly solutions enabled by distributed ledger technology (DLT), is increased transparency (thereby reducing risks of fraud, money laundering, counter terrorism financing, tax evasion, non-compliance with sanctions etc.).

Such developments may also give rise to privacy concerns. In the context of CBDCs, there may be concern about domestic surveillance.

Any digital solution that retail consumers would be willing to adopt will need to comply with relevant data protection laws which needs to be considered from the outset in the design stage. Also to be considered is the level of control any such payment tool will give consumers over their personal information (depending on policy approach users can potentially own more or less of the data generated by their interaction with the tool, which may in some circumstances

enable monetization of valuable spending habits data and so on, features that cannot be replicated at present in traditional systems. Giving back control of data to consumers may also help with building trust).

Encryption and other privacy-preserving technologies can allow for the secure use, transfer and sharing of transaction data. There may be opportunities in the technology behind programmable payment solutions to embed certain rules, in order to automatically prevent unauthorized sharing of data when a transaction is made with the relevant instrument.

We explore digital identity and privacy further in [chapter 3](#).

B. Singleness

The “singleness of money” refers to the need for money to remain as a defined, unambiguous unit of account – i.e. whether we hold our money in bank accounts, notes and coins, we can trust that all has the same value – the pound in my bank account equals the pound in your account. Wholesale central bank money plays a key role in achieving singleness.

The importance of “singleness” in any digital payment/money solution is recognized around the world.

For example:

- [The BIS](#) recently has discussed this in the context of stablecoins and tokenized deposits, where both are forms of private tokenized money representing liabilities of the issuer (and the holder has a claim on the issuer for redemption at par value in the sovereign unit of account), but the latter being more conducive to preserving the singleness of money by virtue of using tokenized central bank money (i.e. a wholesale CBDC) as a settlement asset.
- Andrew Bailey from the BoE also expressed, in a [Speech on “New prospects for money” \(10 July 2023\)](#) that digital money in the form of stablecoins currently fails the basic test of singleness. With respect to systemic stablecoins: “*We will shortly set out proposals for regulating systemic*

stablecoins, under powers contained in the Financial Services and Markets Act 2023. Such stablecoins will have to meet the tests of singleness of money and settlement finality”.

- The Monetary Authority of Singapore highlights the need for singleness in its whitepaper on [Standards for Digital Money](#).

In any new form of digital money/payment solution, singleness of money needs to be preserved. It should be the functionality of the money (i.e. what we can do with it) that is developed and improved, rather than the value of money. Whilst this is not necessarily a set of features that consumers need to understand, digital payments developers and issuers need to stay abreast of the rapidly evolving regulatory environment in this space to ensure that they are building compliant and future-proofed solutions that will be able to last in order that trusted adoption can be built over time.

C. Settlement Finality

To achieve settlement finality means knowing that when we pay for something we can rest assured that it actually has been paid for – any new form of digital payment will need to allow for settlement finality.

Popular non-bank stablecoins cannot offer settlement finality in “real” money – however, this is still a developing space. New forms of digital payments can leverage technology that potentially offer settlement finality more efficiently than traditional systems. For example, the BIS has discussed the theory of a “unified ledger” in its report on a “Blueprint for the future monetary system” – this envisions interlinking central bank money, tokenized deposits and other tokenized assets thus allowing settlement finality while leveraging the technology efficiencies of tokenization.

D. Functionality and security

For any form of digital payment solution to be successful, there needs to be trust in the functionality of the system and there also needs to be trust in the security of the system to prevent hacking, identity fraud, theft, etc. Essentially appropriate technological and operational

controls must be in place to ensure consumer protection.

The digital payments space has experienced some very well-publicized failures, these create “trust barriers” which then need to be additionally overcome in order to move forward. In the context of DLT-based payment solutions, multiple cases of the collapse or unpegging of private stablecoins in recent years has led to

public distrust in stability of private stablecoins, which is unlikely to be overcome for a number of years. However, CBDCs, bank-issued stablecoins or tokenized bank deposits may ultimately lend more credibility and be potential candidates as a trusted instrument to be used as a payment solution.

Key recommendations

1 Any new form of digital money will need to preserve the singleness of money and allow for settlement finality. Developers and issuers need to be fully aware of the complex evolving policy and regulatory environment, including on an international basis where cross-border solutions are being contemplated.

2 Digital payment solutions will need to have implemented robust security measures and ensure operational resilience, such that there is no greater risk (or less risk) to client funds relative to traditional forms of payment (whether this is in relation to the value of the instrument, risk of fraud, or other system failure). Where digital solutions can help to enhance protections, such as better anti-scam checks and tracing for recovery of lost or stolen assets, these features should be prioritized for development. Any developer of digital payment solutions will need to consider data privacy issues and compliance with data protection laws at the design stage.

3 The digital payments space as a whole needs to be careful to consider financial inclusion, usability and simplicity in systems that may be adopted at scale. Similar to the phased approach for the introduction of mobile telephone card wallets and mobile phone payments, where payment limits were initially very low and then subsequently increased, similar staged implementation should be considered so that trust can be built steadily, without risk of major errors and losses arising.



Digital Insurance

Smart contract risk permeates the on-chain economy and remains one of the primary limitations on wider adoption of blockchains today. In this chapter, we review three different paths through which the smart contract insurance industry can grow and mature.

Authors



Nicola Evans
Partner
London



Bryony Widdup
Partner
London



Dave C. Marley
Senior Associate
Philadelphia

Introduction

Much of the on-chain economy runs on smart contracts. The automation provided by smart contract operation is sometimes said to offer “trustless” solutions, meaning that the absence of a third party intermediary who is performing a function obviates the need to trust someone for effective, accurate and timely performance. Automatically executing code fulfils this instead. Decentralized finance applications, non-fungible tokens, decentralized identity solutions, stablecoins, oracles that bridge real-world information to the blockchain and a variety of other aspects of on-chain activity rely on smart contracts functioning as intended. As a result, “smart contract risk” – the risk that smart contracts do not function as intended (whether as a result of a bug, hack, external dependency failure or something else) – permeates the on-chain economy. “Trustless” can become untrusted very quickly when an issue arises and disintermediated automation means there may be no party available or able to step in and prevent a failure. This is one of the primary limitations on wider adoption of blockchains today. Despite the systemic importance of this risk, the market for insurance and insurance-like solutions covering smart contract risk is relatively small and immature. Instead smart contract risk is primarily mitigated by technical mechanisms (like smart contract audits) and incentive mechanisms (like bug bounties). The widespread availability of insurance to cover

losses caused by smart contract failure could clearly help build better trust, and below we consider three different paths through which the smart contract insurance industry can grow and mature.

Bug bounties are rewards offered to third party security researchers (sometimes called “white hat hackers”) for finding and reporting protocol vulnerabilities.

Analysis: Insuring the smart contract

Currently, most smart contract insurance is purchased by the end-user. An individual or organization that holds tokens deposited in a smart contract might, for example, purchase insurance cover to protect against those assets being drained through an error in the code. The user is insured, but the smart contract usually is not. In certain circumstances, however, it may be more efficient to insure the smart contract itself or, at least, to offer end-users the ability to opt into the insurance simultaneously with the primary smart contract interaction. This “insurance by default” model should result in more risk being covered and, consequently, create a larger market that is more attractive for insurers to participate in.

Additionally, insuring the smart contract itself gives the insurer greater control over the risks it is covering. Most reputable protocols subject the protocol’s smart contract code to one or more smart contract audits to identify and fix bugs or other vulnerabilities in the code. Insurers that propose to cover the smart contract itself can partner with the smart contract development teams prior to launch and participate in the auditing process. This early involvement would aid the insurer’s underwriting process, make integrating insurance into the protocol more economically viable and ultimately provide an effective, low cost trust solution to smart contract risk.

Increasing specialization

Participants in the traditional insurance market are highly specialized. Different insurance companies service different lines of business and have geographically distinct market focus. There are also reinsurers, brokers, agents and other industry participants that specialize in serving different clients, risks, geographies and layers of the risk stack. The smart contract insurance market has not yet developed this specialization. Instead, a single insurer may bear the entire risk of loss for a variety of adverse events that could occur with respect to a single smart contract.

However, smart contract risk is not a single type of risk. Consider three recent prominent loss events:

- the Euler Finance hack, which is generally thought to be the result of a vulnerability in the design of the smart contract's source code;
- the Curve Finance exploit, which was the result of a compiler bug (rather than a bug in the source code); and
- the collapse of Terra Luna and its associated stablecoin, which is generally blamed on an economic attack or a weakness in the design of the protocol itself.

The expertise needed to underwrite the risk of the particular loss event that occurred in each case was different. The smart contract insurance market will mature as different participants specialize in underwriting different risks, as reinsurers enter to provide the capital necessary to cover those risks and as brokers emerge to facilitate the placement of a comprehensive insurance product.

Compiler risk is the risk that a vulnerability exists in the program that translates ("compiles") the source code for a protocol into machine-readable code. As many different protocols may rely on the same compiler, compiler vulnerabilities have the potential to result in more systemic losses than source code vulnerabilities (which, generally, will affect only an individual protocol). However, the underwriting burden of assessing compiler risk should also be substantially lower than it is for source code risk as the assessment would not need to be duplicated for each protocol.

Obtaining legal clarity

Although legislation, regulation and case law regarding digital assets and on-chain activity is developing in different jurisdictions, there remains significant uncertainty regarding how the industry will be integrated with the traditional legal system. Consider the following:

1. Are insurers that advise on the audits conducted for a protocol responsible for ensuring that the protocol functions consistently with anti-money laundering laws? What if the insurers underwrite the insurance embedded in the protocol?
2. If a smart contract insurer holds governance tokens in the protocol or votes on decisions affecting the protocol, is the insurer part of a general partnership and liable for the protocol and the acts of other participants? What if insurance is integrated into the protocol itself and the insurer is only making coverage decisions?

The answers to these questions and a variety of others are unclear in many jurisdictions. Given this legal uncertainty, it is unsurprising that the smart contract insurance market has been slow to mature.

Converging paths

We expect that progress in the digital assets market with more comprehensive insurance, increased specialization and enhanced legal clarity will reinforce and build upon each other. As disparate court decisions are harmonized or superseded by a comprehensive legislative framework for on-chain activity, for instance, insurance market participants will be encouraged to work more closely with protocols. As those protocols integrate insurance coverage, the overall market for smart contract insurance will grow and, in turn, create an opportunity for insurers to specialize in different aspects of the market. Of course, this progress is not inevitable and it requires the efforts of a wide variety of contributions to create trust and efficiencies as the fuel in the machine. We need smart contract engineers to develop viable products, confident financiers to fund them, insurers that make those products safe to finance and use, brokers and reinsurers that facilitate the placement of that insurance and lawyers and regulators that work to foster the many different participants in that market.

Further reading:

- [Custodial risk mitigation in traditional and decentralised finance – Hogan Lovells Engage](#)

Key recommendations

1 Insurance by default

It may be more efficient to insure the smart contract itself, or offer end-users the ability to opt into the insurance simultaneously with the primary smart contract interaction. Insurers covering the smart contract itself can partner with the development teams to aid the insurer's underwriting process.

2 Increasing specialization

The smart contract insurance market will mature as different participants specialize in underwriting different risks, as reinsurers enter to provide the capital necessary to cover those risks and as brokers emerge to facilitate the placement of a comprehensive insurance product.

3 More legal and regulatory clarity required

Obtaining legal and regulatory clarity in more jurisdictions will undoubtedly help the insurance market in this field to mature.



AI Governance

AI governance is emerging globally as policymakers and regulators aim to make AI trustworthy. In this chapter, we propose a model for addressing the increasingly complex set of new rules in a seamless and consistent way.

Authors



Eduardo Ustaran
Partner
London



Dan Whitehead
Counsel
London

Introduction

Making AI trustworthy has become a core goal for policymakers and regulators globally. In 2021, the European Union introduced the first major legislative proposal for a dedicated cross-sector framework for regulating AI, commonly referred to as the AI Act. Since then, several other proposals and initiatives have been introduced worldwide. The emergence of new regulations in this area is predominantly driven by the policy objective of protecting end-users, consumers and individuals from potential harms arising from the deployment of autonomous and semi-autonomous technologies. Essentially, emerging global AI regulation aims to achieve digital trust.

In practice, this means that organizations developing or implementing AI systems face an increasingly complex set of new rules that require an effective management approach. AI governance has therefore become a pillar for addressing these rules in a way that enables AI technology to be successfully deployed in a legally compliant way. Doing this at a global scale requires vision and the implementation of practices that are aligned with business objectives. We have developed a model that is specifically aimed at meeting this need in a seamless and consistent way.

“

AI governance has therefore become a pillar for addressing these rules in a way that enables AI technology to be successfully deployed in a legally compliant way. Doing this at a global scale requires vision and the implementation of practices that are aligned with business objectives.

”

Analysis: How can organizations successfully deploy AI technology at a global scale in a legally compliant way?

Potential risks widely regarded as capable of eroding trust in AI include:

- **Algorithmic bias** – The potential for outputs from an AI system to be biased in a way that results in unfair or unlawful discrimination against specific groups or individuals.
- **Opacity** – Due to model complexity, operators of an AI system or individuals impacted by its outputs may find it challenging to understand and interpret the rationale for those outputs in a given context.
- **Performance** – Unanticipated inaccuracies, unreliability and other performance issues may arise, and even go undetected.
- **Misinformation & disinformation** – Content produced by generative AI can misinform due to performance issues. Equally, a model may be intentionally manipulated to produce false or inaccurate content used to spread disinformation.

- **Security attacks** – Bad actors may seek to launch attacks against the AI system, aiming to gain access to confidential information or personal data, or manipulate the system’s behavior.
- **Safety** – Performance issues and malicious attacks can, in certain contexts, result in the AI system becoming unsafe. When the system operates in a physical environment, such safety concerns could pose risks of injury or death to individuals.

In light of this, policymakers across many jurisdictions are focusing on introducing principles and obligations for developers and deployers of AI that are broadly similar. Our recently published [global survey of AI principles](#) identifies eight key areas of focus for policymakers across jurisdictions including the US, European Union, United Kingdom, China, Japan and Australia.

The consistency with which these principles and obligations are being deployed in regulatory proposals allows developers and users to adopt a global approach to AI governance. Simplicity and consistency are key to helping build trust in these systems. Our proposed global approach to AI governance comprises the following core components:

Oversight

To ensure the effective implementation of an AI governance program, it is vital to have adequate oversight and coordination among different departments or teams in an organization. Based on our experience, it is increasingly common practice to establish an AI governance committee (or similar) responsible for providing direction, setting objectives and managing overall enterprise risk.

It is also advisable to undertake an independent audit of existing compliance standards (under legal privilege) in order to identify gaps and inform future priorities.

Responsible AI by design

To comply with many of the obligations proposed under emerging AI regulations, it will be necessary to integrate various technical governance measures into the design, development and deployment of AI tools. These measures are intended to help mitigate the risks we have identified above and “responsible” AI means trustworthy AI. They include:

- **Data governance** – Taking appropriate steps to assess the quality of training and testing data sets and interventions to address potentially harmful biases.
- **Explainability** – Integrating explainability features into AI models to allow for easier traceability of outputs.
- **Performance and accuracy** – Ensuring that models launched into a live production environment perform as expected and, where feasible, address inaccuracies.
- **Robustness** – Addressing the risks of third party malicious attacks on models, which may result in data leaks or manipulation of an AI system.

Documentation

To set consistent standards, demonstrate accountability and provide evidence of responsible AI deployment, it is important to produce appropriate documentation. This may include internal policies and procedures, AI impact assessments and technical documentation. Impact assessments are likely

to form a particularly important tool in risk management, providing a basis for documenting potential risks and mitigations in relation to AI models.

Quality assurance

A key component of the AI Act is ensuring the consistent performance of AI systems throughout their lifecycle and promptly detecting and addressing issues when they arise. Implementing appropriate human oversight, such as testing and ongoing monitoring of systems, is necessary to detect inaccuracies, errors, unexpected behaviours and potentially harmful biases. Employees should receive training on internal AI governance practices to maintain consistent standards throughout the organization.

Transparency

Regulations may require providers to develop detailed user instructions for AI deployers, including outlining how it should be operated and any limitations of the technology. End-users should also receive information about how models operate and that they are interfacing with artificial intelligence.

Liability

In addition to the emergence of new AI regulations, certain jurisdictions are also considering rules for the allocation of liability for faults and damage caused by AI systems. This includes the EU’s AI Liability Directive, which is currently being negotiated. Therefore, it is important to assess whether existing contractual protections are sufficient and whether disclaimers or exclusions should apply to the use of systems in particular environments or for specific high-risk purposes.

Ultimately, AI governance is about understanding the objectives of policy makers and legislators and deploying effective and transparent practices that can maximize the benefits of AI and minimize risk in a lawful and ethical manner. This is essential to responsible deployment and establishment of trust by demonstrating safe application of the technology over time.

Key recommendations

1 Undertake a global regulatory applicability assessment

To understand the full impact of emerging AI regulations, we recommend performing a global regulatory assessment. The objective would be to identify the potential applicability and impact of any proposed laws both to an organization’s existing and potential future projects.

2 Perform a compliance assessment

Considering the applicable requirements, a compliance assessment should be performed to identify current practices already in place, those that are existing and on the horizon (e.g., data governance, bias mitigations, etc.) that can support future adherence to AI regulations.

3 Implement an AI impact assessment tool

This tool should be used to perform and document risk assessments related to existing AI systems and should also be deployed for future solutions being designed and developed. As mentioned above, responsible AI programs involve embedded audit and feedback loops which allow risk identification and mitigation not just in theory, but live and in practice. The importance of impact assessment tools, together with appropriately structured organization level governance to review, understand and act on assessment outcomes, cannot be over-emphasized.



Cybersecurity

Consumer faith in cybersecurity is essential to establishing trust in the digital environment. But with cyber-attacks becoming increasingly common, how can companies ensure their preparation and response to a threat doesn't negatively impact the level of trust placed in their organization? Below we provide a step-by-step guide to the first 24 hours of incident response.

Authors



Nicola Fulford
Partner
London



Vassi Iliadis
Partner
Los Angeles



Paul Otto
Partner
Washington, D.C.



Nathan Salminen
Counsel
Washington, D.C.



Morgan N.G. Perna
Senior Associate
Washington, D.C.



A.J. Santiago
Associate
Washington, D.C.

Introduction

It's 10:00 p.m. on a Friday night. You get a call from your IT department informing you that your organization has been hit by a ransomware attack that has significantly disrupted business operations. A wave of anxiety hits; you begin to feel overwhelmed. You know you need to act, but you don't know where to start. What do you do?

In today's cyber threat landscape, situations like this are increasingly common. For most organizations, it's no longer a question of if the organization will suffer a cyber-attack – it's a question of when. And, of course, the inevitable uncertainty of how you will fare in the face of it. As a result, it is critical to be prepared.

Making thoughtful choices in the initial 24 hours following discovery of a cyber incident can determine how smoothly – or rocky – the next days, weeks, and months will go. Oftentimes, the negative fallout of an incident can either be significantly mitigated or greatly exacerbated in the immediate aftermath; it is imperative that legal teams know the appropriate steps to support their organization during this critical period.

Analysis: What are the critical steps that legal departments must take during the first 24 hours of cybersecurity incident response?

Contact external legal counsel

For more significant cyber-attacks, one of the first steps that an organization should take, during the first 24 hours, is to engage their external cybersecurity counsel to advise on incident response strategy and to maximize the privilege that can be asserted over communications and documents relating to the incident.

Outside counsel can guide you through every step of the process, helping your organization define and implement the various workstreams, timing, and risk considerations appropriate for the particular incident. The Hogan Lovells global incident response team has accumulated extensive experience across thousands of incidents, and can bring invaluable foresight that will help your organization avoid costly mistakes. It is vital to engage experienced external counsel to guide you through this critical 24-hour period and beyond. (And later in the process, outside counsel can help you identify contractual and

legal notification obligations that may have been triggered by the incident and prepare notifications to regulators, customers, and individuals.)

Launch a privileged forensic investigation

Once a cybersecurity incident has been detected, it is important to quickly learn about what happened, where it came from, and the extent of compromise, while also confirming that the incident is contained, the attacker is eradicated, and damage is mitigated.

For more significant incidents, your outside counsel should quickly engage third-party cybersecurity experts to conduct a forensic investigation under privilege. Having the investigation directed by external legal counsel will help to bolster claims that forensic findings, reports, and communications related to the incident are protected by the attorney-client privilege and work product doctrine, which will be critical if the incident results in litigation and also may be helpful for regulatory enforcement.

Assess insurance coverage

Cybersecurity incidents can be costly and some insurers require that you notify them of incidents quickly. Your organization will want to quickly identify any possible insurance policies that may provide coverage. Counsel can help you assess your policy and, if applicable coverage exists, notify your insurer of a potential incident.

Throughout incident response, your insurer may request certain information, and external legal counsel can help you present the incident accurately in a way that minimizes exclusions.

Develop a communications strategy

Perhaps a cybersecurity incident has brought a business function to a screeching halt and your customers are asking questions. Or perhaps a threat actor has identified your organization as its victim or publicly leaked your data online. In these and many other scenarios, you will want to quickly develop a public relations and communications strategy to address inquiries from customers, employees, the media, and other interested parties. External legal counsel can help you do so in a way that addresses these parties' concerns while helping you avoid making statements that could increase the risk of litigation or regulatory enforcement actions down the line.

Consider engaging a negotiation vendor

In the event of a ransom demand, you may want to consider engaging a specialized negotiation firm. Even if you do not want to pay, you should discuss options with outside counsel, as often the negotiation process can be a useful way to gain information or delay destructive actions by the threat actor.

Consider contacting law enforcement

Consider contacting law enforcement to gain intelligence about your attacker. In the case of ransomware, it can be especially helpful to contact law enforcement, as the large ransomware gangs typically have the full attention of dedicated law enforcement teams who can provide significant information and recommendations, and, in rare cases, can sometimes even assist in retrieving stolen data or cryptocurrency, or providing decryption tools. In cases where an organization is considering paying a ransom, it is even more important, as working with law enforcement can mitigate risk that you may be paying a sanctioned party. In some cases, insurers may also require that the incident be reported, and regulators and consumers tend to regard this positively.

So how can your organization best prepare to execute these steps when an incident occurs?

BE PREPARED. You can take steps today that will pay off down the road.

Key recommendations

1 Line up your outside vendors in advance

In the valuable time following an incident, don't be stuck shopping for vendors you're comfortable with and standing up new contracts. Establishing a relationship with outside counsel and other experts *before* an incident starts will allow your outside advisors to hit the ground running in the wake of an incident.

2 Inventory contracts with customers and business partners

Identifying agreements with notification requirements in advance will make it easier to assess what contractual obligations may be triggered by a given incident. You might also identify VIP customers or business partners to help prioritize contract review and communications ahead of time.

3 Prepare, practice, and refine your incident response process

An effective, tailored, and current incident response plan will unite your organization's internal functions to efficiently manage an incident and minimize damage. Outside advisors can help prepare the documents that will guide your internal stakeholders to properly execute their incident response roles and make sure the right decision points are raised and steps are taken at each juncture. Being confident that your incident response plan is effective in the face of an incident benefits from regular testing and refinement of the plan in advance of an incident. Hogan Lovells can assist with this preparation.



Digital Gaming

The gaming industry is far ahead of many digital business models, encouraging users to create and upload their own content and become fully immersed in the virtual experience. For the system to work smoothly, robust frameworks that underpin digital trust and protect IP rights are essential so all parties can safely co-create.

Authors



Anthonia Ghalamkarizadeh
Partner
Hamburg



Janis Beckedorf
Associate
Hamburg

Introduction

The global gaming industry keeps growing and evolving at a rapid pace and fuels highly innovative digital business models. Whenever new technological developments become the talk of the town – metaverse, NFTs, virtual reality and AI – the gaming industry is already implementing them. Allowing and encouraging users to create and upload their own content, to become fully immersed in a 360 degree virtual experience, is an increasingly integral part of gaming. The creation of User-Generated Content (“UGC”), increases sustained player engagement and retention, and allows users to strongly identify with a digital experience – be it through customizable social media avatars, or with more complex UGC that allow users



to build entire landscapes, create artwork, or program their own in-game games. Adding further layers of digital ownership, games often also allow commercial third parties to advertise and market their offerings within a game – resulting in a multi-stakeholder environment. This trend of increasing connectivity and co-existence of proprietary gaming content, owned and developed by the game publisher, with user-consumer UGC and commercial third-party content, creates new complexity and challenges around protection, ownership and transfer of the underlying intellectual property rights of the different stakeholders within a digital environment. For the system to work smoothly, it becomes fundamentally important that game publishers and platform operators put in place robust terms of service that provide a transparent and balanced legal framework within which all parties can safely co-create. These terms of service also need an accommodating legal environment that is sufficiently robust on digital interactions to function with trust and certainty.

Analysis: How can we enable actors in the digital gaming space to trustfully create digital content?

Digital creation, co-creation and ownership rights

Compared to physical goods, digital items can be easily and rapidly shared, modified, multiplied and disseminated. And throughout

these interactions, digital property increasingly becomes the result of a collaborative process, where players make use of virtual elements created by game developers, by other players or by commercial third parties. These collaborative processes can also be found in various other creative digital environments, from metaverse platforms to social media and digital collaboration platforms (including in financial contexts, as well as more obvious ones like NFTs) and training processes for generative AI models.

Much of the creation and sharing takes place on online platforms that provide the framework, resources, tools and accessibility to other creators and users for multi-faceted digital content. Due to the fact that digital content can have significant value, and because the spread of illegal digital content has a massive potential for harm, it is critical that online platforms provide an ecosystem that is technically, commercially and legally trustworthy and, in which digital creators and their creations can maximize their full potential and enjoy creative freedom within safe boundaries, and where collaborative interactions can thrive. Integral to a safe framework are clear and transparent processes for attributing and protecting intellectual property rights.

Legal Background

Within the European Union, the DSM Directive, together with its national transpositions, has

been aimed at adopting copyright law to today’s digital realities. But the digital age tends to move faster than the legislators: Creations within gaming environments were clearly not on the legislators’ mind, and the provisions are still very much written for the more traditional creations – books, news publications, works of art, music, films and photography. Meanwhile, games present a complex composition of graphics, music, text, film sequences, characters and gameplay, with a plethora of (potential) right holders of copyright, design rights, trademarks and patents.

For online content-sharing platforms focused on user-generated content, the directive clarifies that such platforms must, in principle, obtain licenses for all copyright protected works uploaded by their users. While this provision seeks to strengthen the position of right holders in negotiating the terms under which their works are exploited online, it creates uncertainty for all involved parties in an environment in which – as with gaming UGC – it is often very much unclear whether or not a creation enjoys copyright protection in the first place. Platforms rich in UGC, such as Roblox, are publishing guidelines to aid their creators in determining the boundaries of copyright protection for UGC, and such a collaborative and open approach is well suited for the creative environment gaming platforms are fostering.

The transparency obligations under Art 19 DSM Directive, obligating content sharing platforms and other licensees to inform authors about the modes of exploitation, revenues generated and remuneration due, is particularly ill fitting for UGC-heavy gaming and metaverse environments – even if it does come with some flexible limitations that take into account the nature of the sector in question and the revenue relevance of the licensed works.

All eyes on the terms of service

The uncertainties arising from the divide between copyright protected UGC and lesser forms of digital content, the lack of a universal legal framework for digital creations, and the complexity of video game environments all place a laser focus on the terms of service and policies of gaming platforms, as the most flexible and appropriate framework for regulating the creation, dissemination, transfer and deletion of digital creations. While terms and conditions have been around for a long time, they have historically often been overly tilted in favor of the platform operator, as well as being written from a US-centric perspective. This has been changing fast in recent times, with terms becoming more user centric and permissive, allowing users to freely share and commercially exploit gameplay streaming, Let's Plays (a video (or screenshots accompanied by text) documenting the playthrough of a video game, often including commentary and/or a camera view of the gamer's face), and walkthroughs, and sometimes even to take their digital creations off platform to use and exploit them in other digital environments.

Such a permissive attitude becomes more complex the more different creators come together in a digital environment: Should a gaming platform be able to exploit user-generated content to promote the game? Should users be able to create Let's Plays like they are used to, even if these may well depict the – potentially copyright protected – UGC of others? How should an infringement notice be actioned if it relates only to a part of a complex piece of UGC that was the result of co-creation by several users, or that contains proprietary IP of the game publisher? These examples pinpoint some of the complexities arising in a multi-stakeholder

digital creation environment. Content-sharing platforms profit from prolific creation of user-generated content, so it lies in their own best interest, and that of their users, to put in place robust and fairly balanced terms of service that govern the interactions of creators and the ownership and transfer of their creations.

Among others, the following questions should be considered and addressed:

- What licenses must be given by users and by the platform operator in turn, so that the co creation ecosystem can flourish in an environment of trust? Should platform operators be able to use user-generated content in other contexts, such as across games, or to sublicense it? Should users be able to commercially exploit UGC and gameplay for which they have used the platform's resources?
- How can users be protected when they transfer and trade UGC?
- Should, or must, users receive remuneration for their UGC from the platform in certain circumstances? Is it possible to measure which content generates which portion of revenue? What is “appropriate and proportionate remuneration” in an environment with hundreds of thousands, sometimes even millions, of creators?
- Should there be room for individual contracts with certain super-users or should all be treated equally under the terms of use? Does the platform want to leverage the option of ordering specific content from select users?
- How can platforms and users most effectively identify and combat infringements within the parameters of the newly emerging regulation, including the [EU Digital Services Act](#), which is set to establish a new gold standard for content moderation and transparency requirements? Which voluntary content moderation measures and upload filters should a platform put in place?
- How will the fast-growing use of AI, and corresponding emerging new layers of regulation, impact content creation, content moderation, and questions of ownership?

- To what extent is it desirable and legally practicable for users to build on existing content of other stakeholders within the digital environment when they create UGC? Can terms and policies address all repercussions of such co-creations appropriately?
- And the ultimate question it all boils down to: How does a balanced, fair, safe and transparent environment of rights and obligations between the platform operator and its users look like?

Key recommendations

1 Set the terms for trust in co-creation ecosystems

One size rarely fits all. This is particularly true for UGC-heavy digital environments, such as games and metaverse platforms, where content created by the platform operator is mixed with UGC and other third party content, such as commercial content from brands and advertisers. In these digital environments, robust terms and policies are paramount to regulate the creation, sharing, interaction and transfer of digital content in the absence of comprehensive regulation.

2 Engage in stakeholder dialogue with your peers and with your users

While regulators are playing catch-up (the European Commission, for one, is busy drafting its “Vision for emerging virtual worlds”), multi-stakeholder dialogue and MoUs among game publishers and UGC-focused platforms, as well as close guidance to the community through content policies, FAQs and thought leadership are all vital elements for creating and maintaining a trust-based digital environment of co-creation.

3 Safeguard your underage users

Co-creational and UGC-rich gaming environments are usually particularly attractive to minors – who at the same time are among the most vulnerable users. We are seeing a constant increase in regulatory initiatives globally that centers around minors, including age verification and age gating requirements, parental controls at platform and at device level, as well as CSAM regulation. Building robust and forward-looking safeguards for minors, that anticipate the upcoming regulatory developments, into all gaming environments is key – both for the sake of your users, and for future-proofing your compliance.



Digitizing Employment

There are many aspects to digitization in employment but one of the latest is incorporation of AI to employment and resources applications. AI is being embraced by organizations to perform a range of employment-related functions. In this chapter, we consider how employers can build digital trust when using AI to make or influence employment decisions.

Authors



Ed Bowyer
Partner
London



George W. Ingham
Partner
Northern Virginia



Jo Broadbent
Counsel Knowledge
Lawyer
London



Saydee Schnider
Associate
Northern Virginia

Introduction

According to a 2022 survey from the Society of Human Resources Management, at least 79% of employers use some form of automation or AI in their recruitment and hiring decisions. Using AI to perform a range of employment-related functions, including recruitment, has clear business benefits: technology helps streamline processes, making them more efficient and cost effective, and improves employee productivity by automating routine tasks. Recent exponential growth in employers' use of AI, not just in the U.S. but globally, shows that organizations are embracing those advantages.

However, employers need to balance the benefits of using AI against the potential legal and reputational risks. As Charlotte Burrows, chair of the U.S. Equal Employment Opportunity Commission ("EEOC"), the federal agency that enforces anti-discrimination laws in the U.S., commented recently, "AI and other algorithmic decision making tools offer potential for great advances, but they also may perpetuate or create discriminatory barriers, including in employment."

To be sure, AI, if used effectively, can improve decision making and help reduce the risk of bias in hiring and other decisions by eliminating subjective factors. But AI can also make ineffective or discriminatory decisions – such as by selecting poor-performing job candidates, or by favoring (perhaps inadvertently) job

“

The most obvious way for employers to build digital trust is by ensuring that AI systems used in sensitive personal data scenarios like employment are extremely secure and that they assist in making decisions based on legitimate business criteria, clearly they need to avoid discrimination against job applicants or employees based on legally-protected characteristics such as race, sex, age, or disability and they also need to be effective in making or supporting successful choices. Both the employers and the applicants need to be able to trust the system being used.

”

candidates based on factors relating to race, gender, or other protected characteristics.

Legislators and regulators are starting to recognise the potential for AI to cause harm to employees. In some regions, governments are imposing restrictions on employers' AI use, such as New York City's recent [Automated Employment Decision Tools Law](#). [Read more here](#). More commonly, at least for now, regulators and individuals are relying on existing discrimination and data privacy laws to challenge AI-influenced decisions and to require greater transparency about their use.

Analysis: How can employers build digital trust when using AI to make or influence employment decisions?

The most obvious way for employers to build digital trust is by ensuring that AI systems used in sensitive personal data scenarios like employment are extremely secure and that they assist in making decisions based on legitimate business criteria, clearly they need to avoid discrimination against job applicants or employees based on legally-protected characteristics such as race, sex, age, or disability and they also need to be effective in making or supporting successful choices. Both the

employers and the applicants need to be able to trust the system being used. Relying on output from AI systems to make employment decisions can lead to discrimination in several different ways. For example, using a recruitment tool that treats some candidates less favorably based on a protected characteristic, or that sets a quota of ensuring certain numbers of individuals of a protected characteristic will be selected by the tool, is disparate treatment (under U.S. law) or direct discrimination (in the U.K. and Europe).

A milestone settlement recently reached by the EEOC over AI discrimination in hiring highlights these risks. In that case, which settled for US\$365,000, the EEOC alleged that a company programmed its AI-powered application software to automatically reject female applicants over the age of 55 and male applicants over the age of 60. However, even when systems are not designed to intentionally discriminate, problems can become embedded in AI systems in unintentional ways.

For example, data used to train AI tools may not be statistically balanced, or may even reflect past discrimination, which may unintentionally lead an AI to favor or disfavor certain groups on the basis of a protected characteristic. They can also lead to disparate impact (indirect discrimination in Europe) if outcomes put people who share a protected characteristic at a disadvantage, even though the AI tool is not specifically taking the characteristic into account in its decision making.

[Read more in our Employment Horizons 2023 brochure](#)

If an employer identifies unjustified disparate impact, it may be difficult to practically or legally adjust an AI system to remove that disadvantage. Where AI involves machine learning, it can be hard to identify why an algorithm or the training data is causing the relevant effect, which makes correcting it problematic. Additionally, an employer may face claims of discrimination by trying to “fix” a potential disparate impact caused by AI by reprogramming the tool to favour the disadvantaged group based on a protected characteristic, such as having different “pass marks” based on protected characteristics to equalise successful male and female candidates, or establishing a quota based on protected class status.

Another potential risk arises if AI systems put employees with a disability at a disadvantage. For example, an AI-assisted interview that uses visual or verbal data to make hiring recommendations may disadvantage candidates with some types of disability. In that case, the employer may be under a duty to make a reasonable

accommodation/reasonable adjustment to ensure that systems do not disadvantage candidates with disabilities in that way.

Above all, this is an area where governments and regulators are aware of the issues but struggling to keep up with advances in technology. Individuals are becoming increasingly alive to the potential risks of AI and the routes available to challenge decisions they disagree with. Over the next few years, the law will likely begin to catch up, so employers should monitor developments closely.

Ultimately, biased systems that are subject to consistent successful legal challenges, or insecure systems that are subject to data breaches and cyberattacks, will never be trusted. So, it is vital to get all of these features right in any system that is deployed in the employment context.

Key recommendations

1 Algorithms

Ensure algorithms do not rely on discriminatory assumptions, which may require the involvement of multiple individuals during a design phase to identify potential issues before they become baked in and review algorithmic training data to ensure it is representative.

2 AI systems

Monitor the ongoing security of AI systems to avoid data breaches, potential manipulation and other security issues, together with monitoring the output of AI systems to check for potential disparate impact and adjust systems as appropriate and without engaging in disparate treatment by virtue of any such adjustments to reduce any such discriminatory impact. Document the business reasons for using relevant AI systems and explain why alternatives would not achieve those objectives to support a defense to any potential disparate impact claim.

3 Applicant and employee accommodations

Consider – possibly with input from accessibility experts – whether systems could put employees with disabilities at a disadvantage and ensure that applicants and employees can request a reasonable accommodation in connection with employment or application for employment.



Digital Sustainability

Data is central to everything we do, presenting many opportunities for progress in our digital world. And yet, the question of how to store data raises many sustainability concerns. In this chapter we explore three possible approaches under which the sustainable operation of data centers will be possible in the future.

Authors



Tobias Faber
Partner
Frankfurt

Introduction

Data is everything and powers everything we do, from cloud solutions to 5G real-time communications. However, as our usage of data grows, – the question of how to store this increasing amount of data presents its own challenges.

Data centers are at the core of this solution, and we see an increasing number of newly built data centers (greenfield projects) around the globe, in particular, concentrated in certain hubs (like Frankfurt, Amsterdam or Paris) on Continental Europe. While being an attractive asset class, this trend is also accompanied by sustainability challenges given the huge amount of power and energy consumption for cooling purposes. This can be vividly demonstrated by the example of Ireland. In 2022, according to the Central Statistics Office (CSO), data centers used almost a fifth of the Irish electricity. Furthermore, as a trend it can be recognized that the amount of electricity required by data centers has increased rapidly in Ireland over the past few years. Since 2015, it has increased by 400%. Thus, the question of whether data centers can be operated in a sustainable manner is quite pressing, considering their increased energy demand. Some countries have responded to the increased demand for energy by imposing a moratorium on data center projects. Singapore,

for example, imposed a moratorium on new data center projects in 2019 which was then only lifted in 2022 when stricter sustainability requirements were demanded instead.

Since there is also a political agenda to attract data centers and thereby “control” the storage of data, it is rather unlikely that a country will be able to impose moratoriums in the future. Instead of simply prohibiting data center projects, a solution has to be found for operating data centers in a sustainable manner.

Ireland’s Climate Minister Eamon Ryan addressed the environmental issues evoked by data centers at the National Economic Dialogue by stating that every single data center should come up with flexible systems to deliver low carbon electricity and think of ways to use the waste heat effectively. When it comes to the operation of data centers, the trend in the future must be to move away from the mere consumption of energy to the production of self-obtained energy. Furthermore, the produced thermal energy needs to be used effectively. This chapter will present three – possible – approaches under which the sustainable operation of data centers will be possible in the future, with reference to projects already intended in some countries in this area.

Analysis: How can data centers become a renewable utility?

Option 1 – Producing energy on-site via solar

Purchasing ‘green electricity’ from the grid is considered “state-of-the-art” for most data centers. However, data centers maybe be used to produce energy themselves. If data centers were able to generate at least some of the energy they needed themselves, they would be classified as more sustainable from an ESG perspective. One obvious way to generate energy would be to use rooftop solar panels. Since data centers often have a large surface area, if not hindered by cooling systems or other stability elements, and an increasing number of data centers use solar panels on their rooftop. This, of course, only provides a small contribution to the overall consumption.

Option 2 – Being powered by hydrogen on-site generators

Powering data centers on-site, can be further enhanced by replacing typically gas (or even oil fired) on-site generation systems (which provide emergency power supply in case of a blackout of the grid or in other situations), with hydrogen. We anticipate the first data centers globally, but also in Europe, to use such hydrogen on-site

generators will come to market soon. While such on-site generators are currently only used for emergency situations, the longer term future might be to have larger on-site generator units which may help to close the gap and allow for the (full) generation of energy on-site. This would require hydrogen supply pipelines around data center hubs (as being considered in Frankfurt currently, for example).

Option 3 – To make effective use of the heat generated

The third approach is to make effective use of the heat generated on-site. This can be achieved, for example, by transferring the recovered heat to district heating networks. In January 2023, the Frankfurt-based utility and data center operator signed a memorandum of understanding for a joint project on the sustainable use of waste heat and announced that data centers could provide excess heat to Frankfurt's district heating network. A data center in the Digital Park Fechenheim – currently under construction – could become the first to feed its waste heat into the city-wide district heating network and meet the heating requirements of around 3,600 households. Frankfurt could therefore serve as an example for the effective use of recovered heat in the context of supplying households.

Key recommendations

1

In order to operate data centers in a sustainable manner, the primary goal must be to achieve climate neutrality of said facilities. This requires that the facilities are able to generate on-site energy and the waste of the heat generated through data centers is stopped.

2

Generators which are still powered by gas must be replaced. As shown, many countries have seen the need for action and try to support projects which aim to transform data centers into climate neutral facilities.

3

Science and politics will need to work hand in hand to achieve climate neutrality for data centers.





Digital Health Care

The digital transformation of our health care systems can feel like a brave new world – with equal promise and risk for pharmaceutical companies. In this chapter we look at how digital trust is a crucial consideration when navigating digital health.

Authors



Melissa K. Bianchi
Partner
Washington, D.C.



Fabien Roy
Partner
Brussels



Jodi Scott
Partner
Denver



“

For pharmaceutical companies, a thoughtful approach to implementing digital support across the patient pathway will be an important key to future successes. This will necessarily involve enhancing transparency and trust from the perspective of the patient.

”

Introduction

(Traditional) pharmaceutical companies are accustomed to interacting with patients, doctors, regulators, and payers – most notably in the context of manufacturing small and large molecules and the associated approvals and commercialization of these therapies. But when it comes to digital health, it can still feel like a brave new world. With the increasing emphasis on patient access to technology, such as apps, websites, wearables; personalized treatments; Artificial Intelligence/Machine Learning; virtual clinical trials; and real-world data collection, there is increasing promise – and also risk – for pharmaceutical companies looking to improve both therapeutic outcomes and all user (including patient) experience through these innovative technologies. Many stakeholders are surprised to learn that the use of software can involve a huge learning curve and raise issues historically associated with the development of medical devices. Moreover, many pharmaceutical companies still struggle with how to fit digital products into their business models and into their overall organization, and face potential challenges on the regulatory and liability aspects associated with this digital transformation.

A key consideration in this context is the trust required in digital systems when managing sensitive patient health data as companies will potentially become the holders of vast amounts of such data through the development and management of these digital tools and products.

It is crucial for stakeholders to uphold ethical standards, maintain patient privacy, and avoid undue influence on treatment decisions to ensure patient trust and protect their well-being. For pharmaceutical companies, a thoughtful approach to implementing digital support across the patient pathway will be an important key to future successes. This will necessarily involve enhancing transparency and trust from the perspective of the patient.



Listen to our podcast: [Talking the Cure with Hogan Lovells: Talking the Cure – Discussing Artificial Intelligence in Medical Devices on Apple Podcasts](#)

Analysis: How will pharmaceutical companies and other stakeholders protect sensitive patient health data from privacy and cybersecurity risks?

Aligning expectations

Data usage is driving the future of pharma. The ability to collect, analyze, and use data in new and innovative ways is increasingly essential for developing new treatments, improving patient outcomes, and reducing costs. Moreover, it is

nearly impossible to talk about data these days without recognizing the increasing role of AI. The use of AI-enabled systems that collect, store and/or process sensitive personal data, particularly health information, raise important privacy and cybersecurity concerns. In addition, the use of health data beyond traditional clinical development brings forth the possibility of diverse data health projects with varying partner/vendor relationships.

Managing data risks when pharma meets tech

To manage risk appropriately, pharmaceutical companies need to ensure that appropriate data governance processes are in place to secure the data and protect patient privacy. This is true whether or not AI-enabled systems are in place but risks can be heightened, and can present in novel ways, where they are. Proper data governance processes include, at a minimum, internal training on responsible management of health data, robust and up to date policies and appropriate guardrails guiding external relationships where data may need to be shared, with, for example, a third party app developer cooperating in developing a disease care model.

Compliance with health privacy laws can also raise significant challenges of cross-border coordination. Companies must examine their data flows: who is doing what, where the data comes from, and how it is being used. It is generally best practice to evaluate up front what

the data flows will be (particularly whether the transfers will be within a single jurisdiction or cross-border) rather than having to retrofit later. Also on the theme of cross-border data transfers, the EU General Data Protection Regulation (GDPR) provides an additional layer of complexity in the context of sensitive health data, including an additional look at local implementation for health data hosting. Moreover, considerations around “secondary use” of data, such as for research, innovation, policy making, regulatory purposes, and patient safety, are of increasing concern. This is especially worth assessing in the context of the (proposed) European Health Data Space (EHDS), as we have also recently described [here](#). Furthermore, when AI is involved, there are additional compliance and governance layers that must be added, and [we consider AI more deeply in chapter six](#).

Companies should consider:

- What data is needed to develop and deliver the product/service?
- What is the source of the data used to develop any algorithms and can the rights be secured to use that data for all of the possible uses the company may well have in the future?
- What technology access is needed to gain insights from the data?
- What retention rights are needed in relation to that data, and will these needs change over time as intended uses can evolve?
- Is there sufficient experience in-house to analyze the data or will it be necessary to work with others?
- How will data be used by partner(s) and with what limitations?
- What are the selection criteria for the data?
- Where will the data be stored and transferred (from where to where) and with what security precautions?
- Is additional diligence required due to the involvement of an AI-based system?
- If the resulting software application will be a regulated medical device, what data security features will be required, which standards will apply, what data will need to be generated to demonstrate safety, efficacy and security, and what regulatory authorizations will be needed.
- Notice and patient consent may also be required to ensure the appropriate levels of data protection as patients engage with, and develop trust in, the evolving digital health ecosystem.

Key recommendations

1 Data usage

Data is essential for developing new treatments, improving patient outcomes, and reducing costs. However, with the advent and usage of AI, expectations must be aligned with data privacy and cybersecurity concerns and the rights that are secured for the use of that data both for development of applications and also as the applications operate in the real world.

2 Staying abreast of legal developments

Stakeholders with projects currently under development must stay on the alert across jurisdictions in this rapidly developing area which cut across a wide array of legal areas; all of which are evolving.

3 Stay alert to the challenges of cross-border coordination

Europe’s digital future will be guided by recently implemented regulations – notably the GDPR, Medical Device Regulations (MDR), Data Governance Act (Regulation), NIS2 Directive – but will also be increasingly intertwined with other regulations, including under the AI Act, EHDS, and Data Act. While the U.S. and UK are pursuing contrasting (and potentially less prescriptive) approaches, companies should nevertheless be mindful of possible unexpected extraterritorial ramifications of new guidance. This can be especially challenging given the ability of digital services to travel across borders at the blink of an eye.



Digital Transportation

As autonomous driving technology continues to advance, market acceptance and commercial success will be a dynamic process of escalating layers of trust over time.

Authors



Patrick Ayad
Partner
Munich



Lance D. Bultena
Senior Counsel
Washington, D.C.

Introduction

The automotive industry is engaged in a once-in-a-century change in technology. While the shift to electric vehicles (EVs) has received most of the attention recently, the shift to software defined or connected vehicles is just as profound for the industry and ultimately for the public.

Not long ago, many envisioned a rapid transition to (fully) autonomous vehicles (AVs) with mobility services provided by “robo-taxis.” Technical issues were seen as soluble in the very near future and this capacity would pull along consumer acceptance and regulatory development.

This bold optimism has, in many circles, shifted to almost extreme pessimism as some assume autonomous vehicle investments are, at least currently, a lost cause.

We have long argued that as to autonomous drive technology, the issue is not so much when as where. Robo-taxis will not in the near-to-medium-term be a widely available mobility solution. Yet this reality does not mean that autonomous driving technology is not developing and having a significant impact. AV technology is advancing in off-road application in agriculture and industry. This capacity will further transform as sensors, cameras and LiDAR technology as well as artificial intelligence increase capacity.

Driver assistance technology continues to advance and its on-road applications are

increasingly both more robust and more widespread within new vehicles. This technological revolution is neither as rapid nor occurring where some had expected, but that does not mean this technology is not continuing to both develop and transform the on-road driving experience.

Analysis: Automotive and Mobility Sector

A Once-in-a-Century Change in Technology

Most industry analysts expected significant challenges with the fundamental shift in the driving experience and new sources of revenue enabled by connectivity, sensors, and software. The challenges that most focused on were the technology and its capacity. While fundamental, those challenges were – and are – only part of the story.

Taking a profound shift in technology into the mainstream is always a complex undertaking, but it is particularly so for the automotive and mobility industry. The industry is massive, operates on a global scale, and is economically important in all major markets. The industry’s size is not, however, in itself the challenge.

Global scale and economic importance mean the industry is the focus of government policy and of activists, and safety and environment related

functions are very heavily regulated in all major markets. Consequently, the industry does not have the luxury of focusing solely on commercial issues by “merely” working to modulate technological development and change while fostering consumer acceptance in a way that reasonably ensures acceptance and profitability. Instead, government policy is a constant and increasingly significant factor for the industry.

Geopolitical Issues

The automotive industry has always been highly regulated, but geopolitical factors are now very important in government policy impacting the industry’s core operating parameters. AV and driver assistance technology uses advanced sensors and software and runs on extremely advanced silicon chips. All of these technologies are increasingly the focus of competition and regulation between China and the “Global West.” All want to develop these technologies to develop a strategic competitive advantage for their nation and its “friends” because these technologies are economically important and can have military uses. The advanced sensors and the accumulation of personal information may also be of use to intelligence services so, particularly in China, these technologies and their use are heavily regulated.

The shift to electrification only increases the risks and related regulation, as battery technology is very much dependent on raw materials and

battery cells or modules originated or produced in China. The recent EU/China EV trade case is just one example of this latest trend.

Cybersecurity and Privacy

As advanced driving features expand and connectivity becomes even more robust, vehicles generate ever more massive amounts of data that is economically valuable, at least potentially.

As the value of data expands, so does concern about privacy. Again, government policy is a critical actor. Europe's rules are more rigorous and focused on individuals, and are expected to remain so. China's rules optimize for national security with little real concern for individual privacy. Rules in the US are less aggressive than in Europe but evolving.

With connectivity comes concern about cybersecurity, both to protect sensitive data and to ensure the safe operation of the vehicle. In this area, government policy is again key but reasonably stable over recent years.

Safety, Environment and Consumer Trust

Safety and environment related automotive technology is heavily regulated in all major markets. AV and EV technology presents novel issues for regulators. Each major market is taking a different approach that reflects local structure and needs. These rules continue to develop. Their status and structure are beyond the scope of this publication but meeting local safety rules in a market are not only a condition for bringing technology to market, it is essential to consumer trust and acceptance.

Layers of Trust

While consumer trust is essential to market success, in the automotive industry companies do not get to bring their products and services to consumers until they have cleared many regulatory hurdles after they are confident in their technological solution.

While consumers are accustomed to the risks of driving, profound technological change that removes increasing amounts of their "hands on" control creates a new awareness of risk. Many will gain some comfort from the belief that as cars are regulated heavily they must be safe if these capacities are brought to market.

Still, surveys indicate real apprehension in many. Once consumers experience these technologies and normalize the feeling that they are not performing certain driving functions, or even driving at all, then they fairly quickly become comfortable. That comfort and acceptance will be relatively fragile until broad market penetration is achieved. That foundation of trust could be destroyed if early applications are perceived as dangerous. Market acceptance and commercial success will be a dynamic process of escalating layers of trust over time.

Key recommendations

1

Stay attuned to geopolitical factors which are very important as government policy increasingly impacts industry's core operating parameters.

2

Safety, environment and consumer trust are essential to bringing technology to market. Each major market is taking a different approach that reflects local structure and needs. Attention must be paid to developments in each market.

3

Remember that comfort and acceptance of these technologies will be fragile at first until broad market penetration is achieved.



Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
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
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Center: Berlin

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 2023. All rights reserved. WG-REQ-1096