Societal Impacts: Legal, Regulatory and Ethical Considerations for the Digital Twin

Martin M. Zoltick and Jennifer B. Maisel

Abstract A myriad of laws, rules, and regulations are worthy of consideration for any new and innovative technology, and even more so for one as broad ranging and comprehensive as the Digital Twin ecosystem. A technology like this has the contradiction of open versus proprietary, and all the hybrids in between, because it is in the early stages of its evolution that, in many respects, relies on a combination of existing technologies and innovations. From a legal standpoint, we consider intellectual property rights, including patent, copyright, and trade secret protection, and balancing those rights with the benefits and protections available under contract law. The wide applicability of the Digital Twin to various technologies and fields, such as healthcare, finance, education, aviation, power plants, nuclear reactors, any many more, gives rise to regulatory considerations and ethical concerns. The Digital Twin ecosystem, as applied in these areas and more, requires the collection, processing, generation, and transmission of data subject to regulatory requirements involving privacy and cybersecurity issues, as well as ethical concerns requiring careful consideration of potential bias, trustworthiness, and transparency in the technology used.

Keywords Bias · Compliance · Cybersecurity · Digital twins · Digital twins and data · Digital twin ecosystem · Ethics · Innovation · Intellectual property · Laws · Legal aspects · Liability · Patents · Privacy · Protection · Regulations · Regulatory requirements · Rights · Security · Transparency · Trustworthiness

M. M. Zoltick (✉) · J. B. Maisel
Member, Rothwell, Figg, Ernst, and Manbeck, P.C., Washington, DC, USA
e-mail: Mzoltick@rothwellfigg.com

N. Crespi et al. (eds.), *The Digital Twin*,
https://doi.org/10.1007/978-3-031-21343-4_37

1 Introduction[1]

Innovations challenge the boundaries of our legal system, particularly for intellectual property (IP) rights and the availability of different forms of protection for such innovations. Software is a prime example, and even today, legislators, lawmakers, judicial bodies, judges, and practitioners around the globe struggle with fitting software into the different forms of IP and other protection potentially applicable. Now consider the evolution and advancements made in the areas of virtual/augmented/mixed reality, artificial intelligence, machine/deep learning, internet of things, blockchain, biotechnology, big data and analytics, and quantum computing. These technological innovations present new and continuing challenges from legal, regulatory, and ethical perspectives – often, applying or interpreting laws and regulations drafted and enacted years and, in some cases, decades before such technologies were conceived, let alone developed and deployed. Building and implementing these types of technologies typically involves the collection, processing, generation, and transmission of massive amounts of data, giving rise to cybersecurity and privacy concerns. Introducing aspects of artificial intelligence and cognitive computing further invokes ethical concerns requiring careful consideration of potential bias, trustworthiness, and transparency in the technology.

As detailed in the preceding chapters, the Digital Twin requires a wide array of technologies and applies to a myriad of use cases. Simply put, the Digital Twin will be a technological innovation that will test the bounds of our legal system in many ways. The Digital Twin presents unique challenges, from legal, regulatory, and ethical standpoints, because of the confluence of so many different technologies that likely will be applied across many different subject matter areas, in different geographic locations, and by different business entities, enterprises and individuals. The key, based on the authors' many years of experience navigating these issues for clients developing, implementing, deploying, and/or using large-scale complex systems like a Digital Twin, is to develop and implement a strategic, stepwise approach – often tracking the system development lifecycle – that includes consideration of applicable legal, regulatory, and ethical issues. This approach includes: (1) assessing the availability and different forms of IP protection for the Digital Twin technology, (2) conducting IP due diligence search and review in connection with freedom to operate and IP clearance opinions, (3) assessing and negotiating necessary contract rights and establishing a licensing regime for the Digital Twin technology, (4) identifying and assessing compliance with applicable US and International government regulations, and (5) assessing the Digital Twin technology and, particularly, the data used and algorithms and models applied, for potential bias, trustworthiness, and transparency, and developing a mitigation strategy (Fig. 1).

[1] The information provided herein is for general informational purposes only and does not, and is not intended to, constitute legal advice.

Fig. 1 Implementing an IP strategy

2 Assessing the Availability and Different Forms of IP Protection for the Digital Twin

The first step in assessing the availability and different forms of IP protection for Digital Twin technology is to understand what IP is, the basic forms of IP protection, and what aspects of the technology each is designed to cover. Understanding what IP is starts with the concept of "property." "Property" refers to tangible things or assets (*e.g.,* real property, such as a house, and personal property, such as a car) with rights/interests owned by a person or entity. "Intellectual property" refers to creations of the mind for which a set of rights are recognized under the applicable laws. IP rights are considered intangible assets. The basic forms of IP protection include: (1) patent rights, (2) trade secret rights, (3) copyright rights, and (4) trademark rights. It is important to conduct a critical review of all the different technologies that are part of the Digital Twin and make an informed determination, for each identified technology (*e.g.,* models, algorithms, data sets, source code, processing, inputs, outputs, images, graphics, interfaces, functions, architectures, etc.), which IP category that technology falls within (Fig. 2).

Start building an IP schedule that lists the different technologies identified and provides a corresponding indication of the IP rights intended to protect that technology. Set a schedule for periodic review of the current technologies of the Digital Twin and update the IP schedule as appropriate. This IP schedule can serve as a useful roadmap for ensuring that appropriate IP protection is secured and that informed decisions are made about what IP protection to pursue.

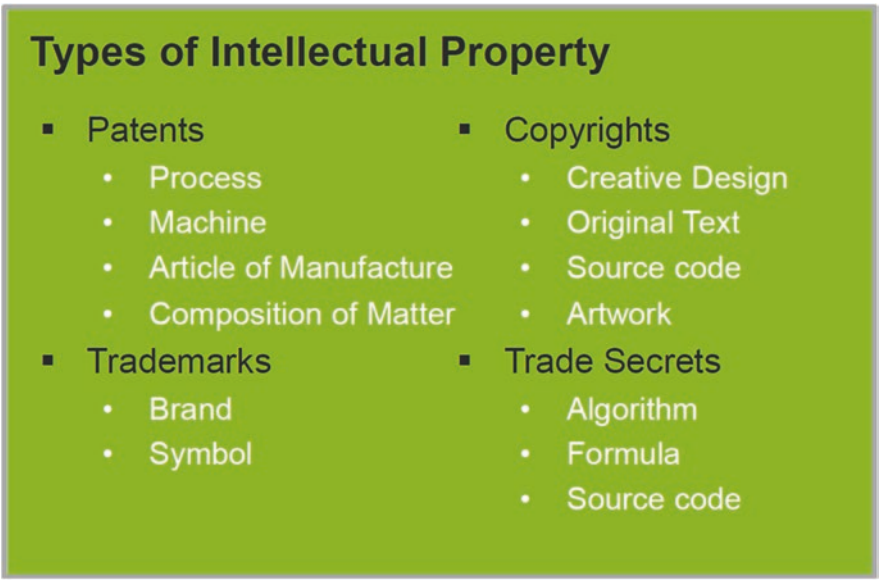

Fig. 2 Types of intellectual property

As a predicate to this process, it is also important for the company to have in place IP policies and procedures to ensure that, for example, any employees of the company or independent contractors engaged by the company working on development of the Digital Twin technology are obligated to: (1) keep company information confidential, (2) disclose to the company all IP developed, (3) assign to the Company all rights in that IP, and (4) not use that IP or any company proprietary information except for the benefit of the company. All individuals working on development of the Digital Twin technology, whether an employee or independent contractor, should be subject to an agreement including these types of provisions. Confidentiality and non-disclosure agreements should be used with any third parties that are provided with access to the company's proprietary information, and all third parties that are involved in the development of the Digital Twin technology should have an agreement with the company that addresses confidentiality, use, ownership and assignment of IP rights, as well as the related provisions typical in such agreements regarding representations and warranties, limits of liability, indemnification, and disputes. Company IP policies and procedures should also include a disclosure process for facilitating the identification and disclosure of innovations to company management, and a defined process for determining in a timely manner whether and, if so, how the company will protect the innovations disclosed.

Also important, particularly in today's development environment, is to have in place guidelines regarding the use of open source and third party software, how to handle adoption and use of standards, and how to deal with data that may, for example, include personally identifiable information or other protected information. Decisions will need to be made early in the development cycle regarding whether

and to what extent aspects of the Digital Twin technology under development will be maintained as proprietary or made open source, and to what extent creation or adoption of protocols and standards will be adhered to. These are particularly important considerations given that the Digital Twin ecosystem relies on a combination of existing technologies and new innovations which, in many if not most applications, will need to be integrated and tightly coupled for data transfer, communications, input/output, etc.[2]

The creation of protocols and standards for the Digital Twin ecosystem to enable plug and play integration for software development and application tools (*e.g.,* Digital Twin simulators, modelers, and viewers), devices (*e.g.,* IoT sensing devices and AR/VR/XR headsets), and digital objects (*e.g.,* cars, planes, boats, condominiums, houses, offices, equipment, clothing, and artwork) have taken on an even greater significance and a broader application with the current hype around the *metaverse*. If the *metaverse* realizes its anticipated potential, the value proposition for the digital objects (and their connected non-fungible tokens (NFTs)) created as part of the Digital Twin ecosystem could be enormous. Indeed, in some cases, those digital objects may realize more value than the physical objects they virtually represent. And, important to that, is the ability to utilize those digital objects across different types of digital platforms.

Establishing protocols and standards for the Digital Twin ecosystem will be critical to enable cross-platform use, and plug and play integration, which will likely have a substantial influence on the overall value of the digital objects, as well as the software development and applications tools and devices used to create and use them. Establishing guidelines for adoption and use of protocols and standards to enable this type of functionality is something that should be considered and decided. One other related legal aspect to mention here is the notion of cross-licensing and standard essential patents (SEPs). The protocols and standards that necessarily will be part of the evolution of the Digital Twin ecosystem and the technology that enables their adoption and use will also necessarily lead to cross-licensing considerations, including the identification of SEPs and the licensing of SEPs under fair, reasonable, and non-discriminatory (FRAND) terms. This consideration should also be part of the IP policies and procedures for the organization (Fig. 3).

[2] The importance of these considerations was highlighted in the current draft publication from the National Institute of Standards and Technology (NIST), NISTIR 8356, entitled "Considerations for Digital Twin Technology and Emerging Standards" (April 2021), p. 4 ("Whether or not these developments catalyze Digital Twin technology into widespread use may depend upon work in standards development. Currently most IoT systems, simulation and modeling software, and VR and AR systems exist in stovepipe proprietary systems. It is possible to combine them, but it takes significant work to integrate them. Much of the work in the emerging Digital Twin area is in the creation of protocols and standards to enable plug and play integration. The idea is to mix and match and be able to use any viewer with any Digital Twin simulator and modeler along with any sensing device. The idea is to be able to load any Digital Twin computer file into a Digital Twin system and have it function regardless of what is being modeled. These are lofty goals for the emerging Digital Twin community; their success in standards may largely determine the extent to which the technology is used.").

Fig. 3 Implementing an IP Strategy: Step 1 – Develop/implement IP policies and procedures

2.1 Patent Rights

Patents rights protect ideas or "inventions." Patents are property rights granted to inventors or, if assigned, to the assignee in exchange for public disclosure of the invention. The categories of patent eligible subject matter include a process, machine, manufacture, composition of matter, and improvements thereof.[3] Laws of nature, physical phenomena, and abstract ideas are not patent eligible.[4] Computerized systems and software-implemented methods may be patent eligible even if directed to an abstract idea[5] if they integrate the abstract idea into a practical application. And, even if the abstract idea is not integrated into a practical application, computerized systems and software-implemented methods may be still patent eligible if they involve significantly more than just the abstract idea.[6] Patent rights represent a

[3] *See* 35 U.S.C. § 101.

[4] See *Bilski v. Kappos,* 561 U.S. 593, 611 (2010; and *Diamond v. Chakrabarty,* 447 U.S. 303, 309 (1980) ("The Court's precedents provide three specific exceptions to § 101's broad patent-eligibility principles: 'laws of nature, physical phenomena, and abstract ideas.'").

[5] There are three categories of subject matter that are considered abstract ideas: mathematical concepts, certain methods of organizing human activity, and mental processes. Only concepts that fall into those groupings can be rejected as "abstract ideas."

[6] The U.S. Patent and Trademark office provides several examples of inventions and corresponding claims that are illustrative of the analysis that is made to determine subject matter eligibility. These specific examples provide good guidance, at least under the current legal standard as applied. *See* https://www.uspto.gov/sites/default/files/documents/101_examples_37to42_20190107.pdf

broader, more powerful form of protection than copyright or trade secret in several respects, which will be addressed in more detail below.

2.1.1 Patent Protection – Digital Twin Examples (From Oil and Gas Projects and Operation)

- Process
  - Advanced analytic engine for a Digital Twin system for predicting corrosion issues using visual and 3D data
- Machine
  - Mobile device with data collection and processing module for inspection using mixed reality (MR) for use with a Digital Twin system
- Article of Manufacture
  - Corrosion detection monitor configured for communication with Digital Twin system
- Composition of Matter
  - Antistatic agent and surface cleaner
- Improvement
  - Improved analytic engine for a Digital Twin system for predicting corrosion issues using machine learning (ML)
- Design
  - New design for smart glasses adapted for use with a Digital Twin system on an offshore production platform

The different types of patents that should be considered relative to securing patent protection for the Digital Twin include: (1) provisional and non-provisional U.S. utility patents, (2) U.S. design patents, (3) Patent Cooperation Treaty (PCT) applications, and (4) ex-U.S. regional and national stage applications and issued patents. There are basic requirements that must be met to obtain patent protection. We will address the requirements under U.S. law, but the requirements in many ex--U.S. countries are very similar. The U.S. Patent and Trademark Office grants patents

---

("Example 37: Relocation of Icons on a Graphical User Interface; Example 38: Simulating an Analog Audio Mixer; Example 39: Method for Training a Neural Network for Facial Detection; Example 40: Adaptive Monitoring of Network Traffic Data; Example 41: Cryptographic Communications; and Example 42: Method for Transmission of Notifications When Medical Records Are Updated."). The European Patent Office has also provided recent guidance on these issues. *See* https://www.epo.org/law-practice/case-law-appeals/communications/2021/20210310.html (PO G 1/19 decision addressing simulation invention for movement through a building.).

for inventions that are new[7] and non-obvious,[8] and that are described in an application with sufficient detail to enable others to practice the invention.[9] The term of the patent is, generally, twenty (20) years from the filing date (Fig. 4).[10]

Patent protection provides the right to "exclude" others from making, using, selling, and offering for sale in the U.S., and importing into the U.S., the invention covered by the patent.[11] This right to exclude is limited to the U.S. If patents rights are secured outside the U.S., then this right to exclude can be exercised outside the U.S. as well, subject to the specific laws in those countries where patent protection has been obtained.

As mentioned previously, patent protection is broader and more powerful than the protection provided by copyright or trade secret. One reason is that, unlike copyrights and trade secrets, patents protect against independent development and reverse engineering. In other words, neither independent development nor reverse engineering is a defense to patent infringement, whereas these are defenses to copyright infringement and trade secret misappropriation. Also, both copyright infringement and trade secret misappropriation require a showing that the accused had access to the copyrighted work or trade secret. Access is irrelevant for establishing patent infringement.

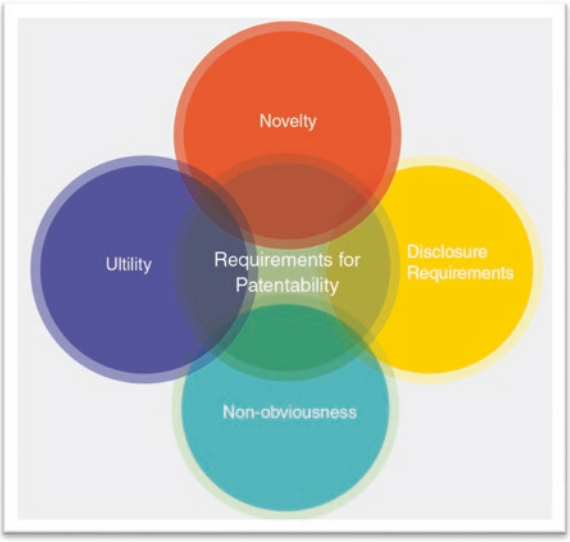

Fig. 4 U.S. Requirements for patentability

[7] *See* 35 U.S.C. § 102.
[8] *See* 35 U.S.C. § 103.
[9] *See* 35 U.S.C. § 112.
[10] *See* 35 U.S.C. § 154(a)(2).
[11] *See* 35 U.S.C. § 271(a).

Autonomous digital agents that can generate new inventions without supervision or input from humans are currently testing the bounds of legal precedent concerning whom or what may be considered an "inventor" of a patentable invention. The creators of the Artificial Inventor Project[12] are actively testing these bounds after filing patent applications around the world in the name of an artificial intelligence creativity machine named DABUS that generated the inventions claimed in the subject patent applications. The United States Patent and Trademark Office and a federal district court recently issued the first decisions[13] in the U.S. refusing to allow the patent applications to proceed because there was no human inventor named.

2.2 Trade Secret Rights

Trade secret rights protect valuable secrets and confidential information against misappropriation and those who improperly derive such information. In contrast to patent rights, trade secret rights do not protect against reverse engineering or independent development. In the U.S., state and federal law govern trade secret rights. State laws vary, including with respect to definitions of what constitutes a trade secret and misappropriation of a trade secret. Federal laws include the Defend Trade Secrets Act ("DTSA"), which provides a federal remedy for misappropriation of trade secrets, and the Uniform Trade Secret Act ("UTSA"), a model trade secret protection framework adopted by most, but not all, states in the U.S. In addition to civil penalties, theft or misappropriation of trade secrets is a federal crime under the Economic Espionage Act. Because of the differing state laws, the company policies and procedures as applied to trade secret protection will need to be tailored to the law of the applicable jurisdiction(s) for the company.

Examples of trade secret information can include software and source code, algorithms, machine learning models and weights, formulas, patterns, compilations of information, data sets (raw, query, training, extracted), technical data, processes, know-how, system architecture, research and development information, technology, designs, drawings, engineering, hardware configuration information, customer information, inventions, unpublished patent applications, marketing data, business plans and strategies, financial information, supplier information, and many other types of information. While an analysis of state and federal law must be done as applied to the company's information and activities to determine whether information would be regarded as a trade secret, a trade secret may be anything that has economic value and provides an advantage in the marketplace. The company must take reasonable steps to maintain the information as a trade secret, otherwise legal protections over the information will be lost (Fig. 5).

---

[12] *See* Artificial Inventor Project, available at https://artificialinventor.com/dabus/

[13] *Thaler v. Hirshfeld*, 20-cv-903 (E.D. Va., Sept. 9, 2021); *In re Application of Application No. 16/524,350*, Decision on Petition (Apr. 22, 2020), available at https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf

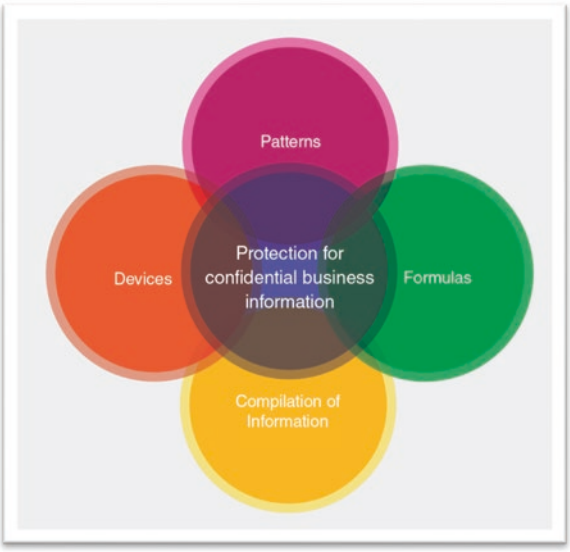

Fig. 5 Trade secret protection

2.2.1 Trade Secret Protection – Digital Twin Examples (From Oil and Gas Projects and Operation)

- Source code
- Machine leaning models
- 3D data
- Architecture for integration of Digital Twin data sources

Trade secrets (whether in electronic or paper form) should be systematically inventoried and documented in a manner that considers the value that the information confers to the company. This is an important part of the process to ensure that the company's trade secrets are properly identified and substantiated, and, if necessary, to prove trade secret status if there has been a misappropriation requiring litigation. Another part of documenting the company's trade secrets is to ensure that all documents in either paper or electronic form including company trade secret information include a notice of confidentiality. An example of such a notice, to be stamped or otherwise applied to the header, footer, or title page of all company trade secret documents is as follows:

> CONFIDENTIAL AND TRADE SECRET
>
> This document contains highly confidential information, including trade secrets, owned by Company and this document and its contents are protected under state and federal law including, but not limited to, copyright, patent, and/or trade secret law. Access to and use of this information is strictly limited and controlled by Company. The receipt or possession of this document does not convey any license or right to copy, reproduce, distribute, disclose, or use its contents in any manner whatsoever without the express written authorization of Company. Copying, reproducing, distributing, disclosing, or otherwise using such information without the express written authorization of Company is strictly prohibited.

2.3 Copyright Rights

Copyright rights protect original expressions of ideas, not the underlying ideas (which, as discussed previously, are subject to patent and trade secret rights, as applicable). Copyrightable works include: (1) label designs; (2) pictorial, graphic, sculptural works; (3) literary works; (4) motion pictures, audiovisual works; (5) sound recordings; and (6) derivative works.[14] Copyright rights are granted to the author of the work or, if made by an employee within the scope of employment or under a contract designating the work as a "work made for hire," to the employer.

2.3.1 Copyright Protection – Digital Twin Examples (From Oil and Gas Projects and Operation)

- Source code
- 3D engineering models
- LiDAR scans

Copyright protection is automatic and established immediately from the time the work is created in fixed form – that is, upon "fixation" of an original work in a tangible medium. Copyright protection is not contingent upon registration, but registration is a prerequisite to suing for copyright infringement and recovery of statutory damages, attorney fees and equitable relief. A copyright endures for the life of the author plus 70 years or, in the case of works made for hire, the longer of 95 years from date of publication or 120 years from creation.

Copyright protection confers upon the copyright owner the exclusive right to reproduce the work, prepare derivative works, distribute copies of the work, display the work, and perform the work.[15] Copyright does not preclude others from independently creating the same work or deriving it by reverse engineering.

As with patent rights, currently in the U.S., machines (and other non-humans) cannot be an "author" of a copyrighted work. This precedent came from a series of cases concerning the copyright status of "selfie" photos taken by Celebes crested macaques (Fig. 6). The People for the Ethical Treatment of Animals (PETA) organization filed a lawsuit on behalf of the 6 year old monkey, Naruto, asserting ownership of the photos. A federal judge dismissed the suit, ruling that animals cannot assert copyright protection, and an appellate court affirmed the decision (Fig. 6).

[14] *See* 17 U.S.C. § 102.

[15] *See* 17 U.S.C. § 106.

Fig. 6 Self-portrait of a female Macaca Nigra (Celebes crested macaque) in North Sulawesi, Indonesia, who had picked up photographer David Slater's camera and photographed herself with it

2.4 Trademark Rights

A trademark identifies the source or origin of a party's goods or services. Trademarks are property rights in marks (*e.g.,* words, names, logos, designs, graphics, interfaces, brands, taglines, etc.) that are used to distinguish a party's products and/or services from those of others. Trademark rights confer upon their owners the right to prevent others from using confusingly similar marks. Under U.S. law, rights in a mark are created by using the mark in interstate commerce. Registration is not required, but registration gives the owner: (1) the right to sue in federal court for infringement, (2) treble damages and attorney fees, (3) a presumption that the mark is valid, (4) rights in a greater geographical area, and (5) a basis for ex-U.S. protection.

A trademark's strength is proportional to the distinctiveness of the mark – i.e., most distinctive are fanciful and arbitrary marks; less distinctive are suggestive marks; even less distinctive are descriptive terms, which must have acquired secondary meaning to serve as a mark; and least distinctive are generic terms, which cannot serve as a trademark (Figs. 7 and 8).

The rights in the trademark will endure so long as the mark is used and does not become generic (Figs. 9 and 10).

With all these different forms of IP protection in mind, the next step is to develop a strategy for IP protection for the Digital Twin technology. A key first step in this

Fig. 7 Fanciful marks and arbitrary marks

Fig. 8 Suggestive marks and descriptive marks

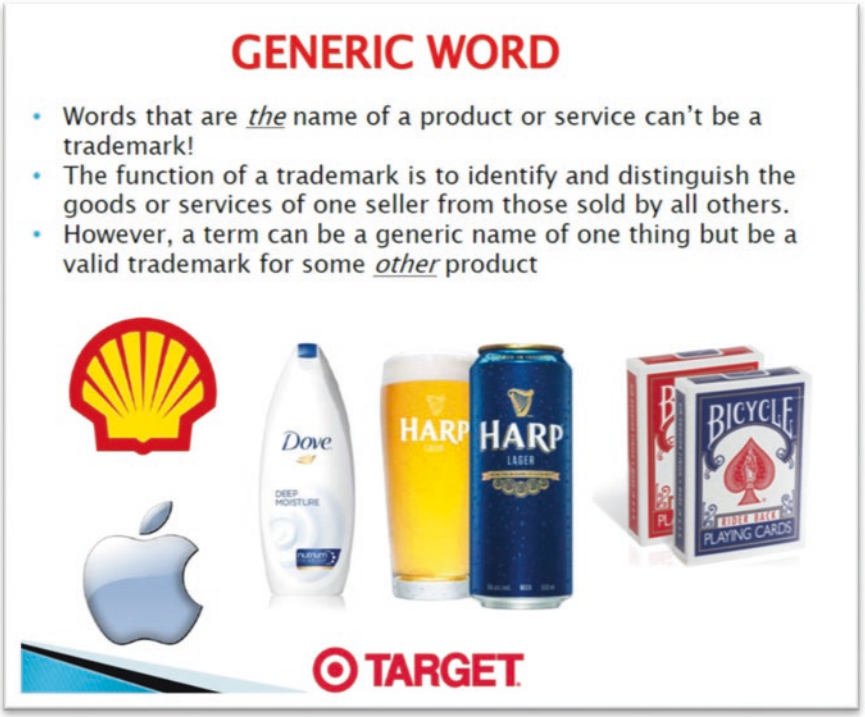

Fig. 9 Generic words

Fig. 10 Trademarks that are now generic terms in the U.S.

process is to conduct a detailed review of all aspects of the Digital Twin technology. This audit should consider all the research conducted as part of the development effort and involve reviewing electronic and, if created, paper records of the employees, independent contractors, and other individuals work in conceiving, developing, prototyping, modeling, coding, etc. the various features, functions, operations, algorithms, interfaces and all aspects of the structure, function, and operation of the Digital Twin technology under development.

From this audit process, the developments – i.e., ideas, inventions, processes, software, products, devices, equipment, designs, graphics, interfaces, compositions, names, logos, brands, taglines, etc. – can be identified and a schedule prepared cataloguing, with appropriate descriptions, the identified developments. In addition to descriptions, documentation supporting the development work should be included (or at least links should be provided if in electronic form) to provide evidence of the development work (*e.g.,* metadata, names, creation dates, locations, specifications, prototypes, flow charts, pseudo-code, source code, screen shots, presentations, etc.). To the extent that electronic communication platforms (*e.g.,* Slack, etc.), source code repositories (*e.g.,* Github, etc.), or other systems are used, extracting development records, or linking to them in the schedule can be very useful for documenting the development work and later preparation of patent applications and other filings, if pursued. Another helpful aspect to include in the schedule is an indication of whether, for each identified development, the work involved a third party and/or was in connection with any work funded by the government or pursuant to a government contract.

With the development work properly identified and documented, company management can undertake a detailed review, typically in consultation with in-house or outside IP counsel, to consider the different forms of IP protection that may be available – i.e., patent, trade secret, copyright, and trademark – and make a strategic decision, based on legal and business considerations, what IP protection to pursue. The legal considerations will typically turn, at least in part, on the subject matter of the development and whether it is the type of technology protectable by a patent or trade secret – like ideas, inventions, processes, software, products, devices, equipment, designs, graphics, interfaces, and compositions – or by a copyright or trademark – like designs, graphics, interfaces, names, logos, brands, and taglines. These are not separate inquiries as, for example, with software, protection may be available by patent to protect the process performed by the software, by trade secret or copyright to protect the source code, and by trademark to protect the graphics, for example. Another legal consideration is based on an understanding of how easy or not reverse engineering of the identified technology is expected to be, timeline for independent development, and whether, ultimately, disclosure of the technology (as a quid pro quo for securing patent protection) or maintaining the technology as a secret is better. From a business standpoint, cost is always an important consideration and, depending on the number of developments under consideration and whether global protection is required or at least desirable, the legal fees and costs can be substantial. Evaluating the status of the company (*e.g.,* early stage or mature, seeking funding, potential merger, or acquisition target, etc.), the competitive

Fig. 11 Implementing an IP Strategy: Step 2 – Develop strategy for IP protection

landscape (*e.g.,* crowded field, mature patent landscape, first mover/innovator, etc.), and the licensing strategy (*e.g.,* does the company intend to license the IP, only for internal use, etc.) are all important business considerations that will, in-part, drive the decisions for IP protection (Fig. 11).

All of this is an ongoing process, and the company should have in place a periodic review procedure (*e.g.,* weekly, monthly, quarterly, as appropriate) to ensure that the company's innovations are given due consideration and a strategic decision is made regarding IP protection.

3 Conducting IP Due Diligence Search and Review in Connection with Freedom to Operate and IP Clearance Opinions

Along with the strategic decisions about IP protection, the company must also consider the risks, from an IP standpoint, of utilizing the Digital Twin technology contemplated. At an appropriate point in the Digital Twin technology development cycle – typically, when aspects of the technology to be used have been tested and there is a plan to utilize that technology in the anticipated or commercial implementation –, the current IP landscape should be searched to determine whether there are any enforceable IP rights that would potentially be infringed by using the contemplated Digital Twin technology. These types of searches are typically referred to as "freedom-to-operate" (FTO) or clearance searches and, along with the search

results, a legal opinion should be given so that the company can assess risk and make an informed decision regarding how to proceed.

One other option to get a sense of the patent landscape earlier in the development cycle is to conduct a patent landscape search that will identify, for a specific technology (e.g., IOT, AR/VR/XR, Blockchain, etc.) in a specific geographic region or country, what the concentration of issued patents and published pending applications is and identify the details for the patents and applications identified (e.g., patent/application number, title, date, inventor(s), assignee(s), etc.). This can be used to identify potential blocking patents and open areas, to assess whether licensing in may be necessary, and to inform whether a change in direction for the contemplated technology is warranted.

As part of FTO/clearance searching, due diligence can be conducted on commercially available technologies, products, software, hardware, devices, etc. that may be used as part of the contemplated Digital Twin technology, as well as on companies, to identify IP rights, licenses, and other legal protections that need to be considered.

There are several available platforms and databases that can be used for these types of searches (*e.g.,* Derwent Innovation, Espacenet, Relativity, InnovationQ Plus, Google patents, USPTO/EPO/JPO and other patent office databases, etc.). The scope, in terms of subject matter and geography, and search logic must be very carefully optimized to ensure that the search results are focused and useful.

With the results of these searches, a detailed review should be conducted, typically by in-house or outside IP counsel, to determine whether any patents identified could potentially be infringed by practice of the contemplated Digital Twin technology and to identify any relevant published applications still in process that should be placed on watch to track prosecution. The opinion provided regarding FTO/clearance should be considered by management of the company in assessing potential risk of going forward with the contemplated Digital Twin technology and determining the basis for proceeding. Clearance searches should also be conducted, and opinions rendered for any trademarks that the company intends to use in connection with the contemplated Digital Twin technology.

With these opinions in mind, and the previous strategic decisions made regarding IP protection, preparation of patent applications, applications for trademark registrations, and applications for copyright registrations should be initiated. To the extent that protection is sought across multiple countries, counsel in multiple countries may need to be engaged and involved in the process to ensure that region- and country-specific requirements and practices are satisfied, and to assist with the filings. To the greatest extent possible, all filings should be made prior to any disclosure of the company's Digital Twin technology to any third party. If this is not possible, the company should ensure that, prior to any disclosure, an appropriate confidentiality and non-disclosure agreement is in place.

After the filings have been made, the IP schedule should be updated to reflect the patent, trademark, and copyright filings, and to identify the developments that the company has decided to maintain as trade secrets. Again, this is an ongoing process, and a periodic review procedure (*e.g.,* weekly, monthly, quarterly, as appropriate) should be followed to ensure that IP schedule is maintained and up to date (Fig. 12).

Fig. 12 Implementing an IP Strategy: Step 3 – Secure IP rights/FTO clearances/opinions

4 Assessing and Negotiating Necessary Contract Rights and Establishing a Licensing Regime for the Digital Twin Technology

It is expected that, with any large-scale complex system like the Digital Twin use cases described in the preceding chapters, there will be many different technologies and entities involved the development process. As such, it is necessary to assess and negotiate the required contract rights to ensure that the company has the necessary rights to use the technologies as needed as part of the Digital Twin. Further, and as discussed earlier as part of the development process, it is important to ensure that confidentiality and non-disclosure agreements are in place with all third parties and that all employees and independent contractors have executed employment and IP agreements assigning all IP rights to the company. Also, as part of the development process, it is likely that some aspects of technology development, testing, prototyping, evaluation, or other activities will be carried out as joint efforts in collaboration with third parties or utilizing third parties as vendors or service providers to carry out certain development-related activities. It is critical to establish the appropriate contract terms with these third parties to address, for example, ownership and assignment of any jointly developed IP, licensing and sub-licensing rights, privacy, and data protection issues, limiting access as appropriate, dealing with timing and schedules, costs, and other necessary terms and conditions of the relationship.

Taking into consideration that the Digital Twin ecosystem will involve many different technologies, applied across many different subject matter areas, in different geographic locations, and by different business entities, enterprises and individuals, the issue of who may ultimately be responsible should a problem, accident, or other issue arise must, at a minimum, be thought through and, in a best case scenario,

decided. While the applicable laws and regulations may determine who has liability, the better approach, at least when the parties involved have some kind of business or other relationship, is to negotiate and agree on who has responsibility and liability.

A party's obligations regarding responsibilities for assessment and enforcement, and exposure for liabilities, should a problem, accident, or other issue arise, can be addressed by contract through provisions that specify which party will have responsibility, who will be liable for things like, for example, patent, copyright or trademark infringement, trade secret misappropriation, product liability and other claims. Contracts between joint developers, licensor/licensee, manufacturer/distributor/end-user, and general contracts between those involved in the Digital Twin ecosystem can include representations and warranties, indemnification provisions, limitations of liability, and enforcement obligations to ensure that there is certainty around who is and is not responsible and liable under the various situations that may arise. These types of contract provisions can provide some needed certainty for companies developing, implementing, deploying, and/or using large-scale complex systems like a Digital Twin.

The company must also consider, in connection with the Digital Twin technology and the IP secured to protect it, how the technology and IP will, if at all, be licensed. This requires an understanding of how the Digital Twin technology developed will be made and used, and whether and how it will be offered (*e.g.,* distributed/sold, available through a subscription, software-as-a-service (SAAS), hosted, etc.). In addition to considering the legal aspects, business aspects must also be considered, such as, licensing fees, the scope of any license or sublicense granted, the term, field of use and territory, whether the license should, or even can, be exclusive, how indemnification will be structured, and the limits of liability. There are, of course, many other legal and business considerations that need to be considered.

If patents will be licensed, it is important to include a patent marking requirement as part of the license agreement to meet the requirements of "constructive notice" to maximize the potential recovery of damages if enforcement of the patent is necessary to address infringement. To the extent that the subject Digital Twin technology uses open source or third party software, the applicable open source and third party licenses need to be reviewed and the requirements for distribution, which may require attribution and making the company's code available (*e.g.,* copyleft licenses like the General Public License (GPL)), must be carefully considered. In addition, if aspects of the Digital Twin technology need to be compliant with standards (*e.g.,* 5G, LTE, 3GPP2, IEEE P2413, ISO/IEC/IEEE 42010, etc.), appropriate representations and warranties need to be included to ensure compliance (Fig. 13).

To round out the company's IP strategy, a plan for enforcement and defense should also be discussed. As part of this plan, the company, either itself or using outside assistance (*e.g.,* IP counsel, private investigator, IP search firm, etc.), should undertake periodic investigations to determine if the company's patents, trademarks, and copyrights are being infringed, any of its competitors are competing unfairly or committing false advertising, its trade secrets have been misappropriated, or its technology is being used in violation of agreements that it has in place. If any of these violations or unauthorized uses are identified, the company should explore its

Fig. 13 Implementing an IP Strategy: Step 4 – Negotiate/execute agreements/licenses

options about potential enforcement, licensing, or other business arrangement to seek to resolve the dispute. If a resolution out of court is not feasible, the company should consider initiating a litigation or contested proceeding, which could potentially be brought in a court (*e.g.,* District Court or equivalent ex-US tribunal), before a government agency (*e.g.,* International Trade Commission, Patent and Trademark Office), or another tribunal. Another possibility is to seek to resolve the dispute by engaging in alternative dispute resolution (ADR), which can be conducted before an organization (*e.g.,* American Arbitration Association (AAA), JAMS, International Chamber of Commerce (ICC), etc.) or by using a private mediator or neutral.

To the extent that the company is accused of violating third party IP rights, a procedure should be established for the company's defense. This should involve a detailed assessment of the alleged infringement or other type of violation and consideration of the validity and enforceability of the IP and the claim. If the claim cannot be satisfactorily resolved through negotiation, the company should consider a proactive approach to challenge the infringement allegation and/or attack the validity and enforceability of the IP through available procedures in the Patent and Trademark Office (*e.g., Inter Partes* Review (IPR), opposition, cancellation, etc.) or in a court (*e.g.,* Declaratory Judgement, invalidation proceeding, etc.) (Fig. 14).

Fig. 14 Implementing an IP Strategy: Step 5 – Develop strategy for enforcement/defense

5 Identifying and Assessing Compliance with Applicable US and International Government Regulations

Digital Twin (DT) technology is not immune from the centuries old conflict between innovation and regulation. DT technology has not been the subject of laws or targeted regulatory scrutiny. For example, in the United States, we currently do not find laws and regulations specific to Digital Twin technology *per se*. Many organizations build and apply DT technology in countless industries in effective, safe, and legally compliant ways, as described throughout the chapters of this book.

DT technology poses unique risks, particularly in view of the data ecosystems that power DT technology, the decentralization and connectivity of DT platforms, and the myriad of applications of advanced DT technology – especially in highly regulated industries. The following section focuses on a key risk area for DT technology: compliance with global privacy and data protection regulations, including heightened security requirements for connected devices.

5.1 Privacy and Data Protection

Personal Digital Twins leverage actual, current, and continuous human data and life history in highly transformative ways. For example, personal Digital Twins are revolutionizing healthcare with digital tracking and advanced modeling of the human body to improve patient outcomes and medical processes. Personal Digital Twin

assistants are anticipating and acting upon a person's needs around the clock. Personal Digital Twins are building bridges between how a person looks and acts in the physical world and across digital worlds in the *metaverse*. Indeed, endless potential applications exist for personal Digital Twin technology that allow persons to experiment with different life choices and explore possible paths to inform everyday decisions.

However, organizations must balance the benefits of personal DT technologies with the privacy rights of individuals, such as the right to be left alone and the right for personal information to be protected from public scrutiny. In view of the explosive generation and utilization of digital data, an increasing number of jurisdictions around the world have imposed privacy and data protection regulations. These regulations affect personal DT technology. Accordingly, consideration of the legal concepts of "information privacy" and "data protection" is important, especially where DT technology leverages data relating to an identifiable person. Information privacy concerns rules regarding an organization's collection, use, disclosure, retention, and disposal of personally identifiable information, as well as any rights an individual has with respect to an organization's collection, use, disclosure, retention, and distribution of that individual's personally identifiable information. Data protection concerns rules regarding the handling, storing, and management of personal information. Intuitively, one cannot have privacy without security, and a key component of privacy and data protection regulations is the requirement that an organization must keep PI/PII, and other sensitive data secure from unauthorized disclosure or use.

We provide an overview of the regulatory framework, and an overview of best practices for regulatory compliance.

5.1.1 Regulatory Framework

Numerous definitions of personal information (PI) or personally identifiable information (PII) exist and generally encompass a set of information that can distinguish or trace an individual's identity. Personal information may include information such as a name and biometric records, alone or when combined with other personal or identifying information that are linked or linkable to a specific individual. Regulators may afford heightened privacy and security limitations to certain categories of "sensitive" personal information, such as financial information, medical records, racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, and biometric data.

In addition, privacy and data protection regulations have two principal categories: general regulations and industry-specific regulations. General regulations apply broadly to processing of any PI or PII, whereas industry-specific regulations target certain covered entities (*e.g.,* banks, healthcare providers) and/or certain categories of PI/PII (*e.g.,* financial records, health records).

General regulations, such as Europe's General Data Protection Regulation (GDPR), define responsibilities for "controllers" and "processors" of personal

information, such as implementing "privacy by default" and "privacy by design," maintain appropriate data security protections, and obtain appropriate consent for most personal data collection and provide notification of person data processing activities, among other responsibilities. Additionally, data subjects (consumers) are afforded certain rights such as erasure, removal (right to be forgotten), access, data portability, and rectification of personal data. Notably, the GDPR also provides data subjects the right to object to automated decision-making processes, including profiling, that affect substantial rights. Many other countries have adopted similar GDPR-like general regulations, such as the Japan Act on the Protection of Personal Information, the Australia Privacy Act, the Brazil General Data Privacy Law, the South Korea Personal Information Protection Act, China Personal Information Protection Law, Canada Personal Information Protection and Electronic Documents Act, among others.[16]

In the United States, a patchwork system of federal and state laws and regulations govern information privacy and data protection. While there currently are no general federal privacy and data protection regulations, several states have adopted such regulations, including California,[17] Colorado,[18] and Virginia.[19] In addition, federal laws (as well as state laws) target the collection of and access to certain types of personal information data by entities in specific industries. Some of the most well-known regulations include: the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act (FCRA), the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), the Telephone Consumer Protection Act (TCPA), and the Electronic Communications Privacy Act (ECPA or Wiretap Act).

There are numerous avenues in the Digital Twin context for an entity to engage in controller or processor activities of PI/PII and therefore be subject to privacy and data protection regulations. For example, application and gaming providers that collect PI/PII directly from consumers and determine the manner in which the collected PI/PII is used, such as building personal digital avatars in the *metaverse*, have obligations as a controller of that collected PI/PII. Similarly, an entity that acts on behalf of such a controller to process the collected PI/PII, such as providing data storage or other services, has obligations as a processor of the collected PI/PII. In some instances, an entity may be engaging in both data controller and processor activities. In distributed Digital Twin systems where, multiple entities are processing PI/PII, a data processing agreement between a data controller and data processor is key in regulating the processing of PI/PII and the obligations of the parties.

---

[16] For a more complete listing, visit the International Association of Privacy Professionals' Global Comprehensive Privacy Law Mapping Chart, available at https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf

[17] The California Consumer Privacy Act and California Consumer Privacy Act Regulations.

[18] Colorado Privacy Act.

[19] Consumer Data Protection Act.

5.1.2 Security of Connected Technologies

Organizations often use DT technology as a platform for Internet of Things (IoT) applications, with uses in smart buildings, cities, transportation, logistics, agriculture, telecommunication infrastructure, and complex cyber-physical systems, among many others. As IoT systems powered by connected devices continues to grow, so do the DT platforms used to replicate, simulate, and manage these complex systems. As highlighted in recent years, IoT systems are subject to unique, and sometimes compounded cybersecurity risks, such as vulnerabilities within IoT devices, lack of physical security over remote devices and weak passwords, insecure data communication and transfer, mismanagement, or lack of visibility of remote devices, and insecure application program interfaces, among others. While many organizations use DT technology effectively to help ameliorate some of these cybersecurity risks, many of the same cybersecurity risks present in IoT systems will also proliferate in the DT platforms used for such systems.

In response to an escalating number of data breaches concerning systems containing personally identifiable information, all fifty states in the United States have enacted data breach notification laws. Additionally, most of the privacy and data protection laws listed above contain data breach notification provisions. Companies may face severe penalties for failing to implement and follow reasonable practices to protect and secure digital devices, software, and systems from data breaches, as well as for failing to properly report covered data breaches. In addition to fines and potential regulatory investigation, companies facing a data breach may be subject to litigation initiated on behalf of individuals – or classes of individuals – that are personally harmed by the breach. For example, members of a class action litigation in the United States against the credit reporting company Equifax were able to receive free credit monitoring or up to $125 cash payment from the company.[20] The litigation stemmed from a 2017 data breach that impacted the personal information of approximately 147 million people.

While there is little "Digital Twin" focus to date, lawmakers and regulators are heavily scrutinizing the broader Internet of Things (IoT) industry. For example, the United States Federal Trade Commission (FTC) has been focusing on data privacy and data protection in the IoT industry and is becoming increasingly aggressive in launching investigations and initiating enforcement proceedings against IoT technology companies. A long line of FTC cases relates to IoT technology, and most recently, the FTC settled an investigation in *Tapplock*. In *Tapplock*, the FTC alleged that an internet connected smart lock provider deceived customers by falsely claiming that it designed its locks to be "unbreakable" and that it took reasonable steps to secure the data it collected from users.[21] The FTC has issued guidelines and

[20] https://www.equifaxbreachsettlement.com/

[21] In the Matter of Tapplock, Inc., available at https://www.ftc.gov/enforcement/cases-proceedings/192-3011/tapplock-inc-matter

recommendations pertaining to IoT platforms, and the FTC's fifth and sixth "PrivacyCon" conferences included discussion on the privacy and security risks of IoT devices.[22]

Additionally, several laws took effect in the United States over the past few years concerning the security of connected devices. California Senate Bill 327, "Security of Connected Devices" specifies the security obligations of manufacturers of connected devices, including equipping devices with reasonable security features. Such security features must be (1) appropriate to the nature and function of the device, (2) appropriate to the information it may collect, contain, or transmit, and (3) designed to protect the device and any information contained thereon from unauthorized access, destruction, use, modification, or disclosure. Oregon House Bill 2395, "Security Measures Required for Devices that Connect to the Internet," is like California's law.

At a federal level, the IoT Cybersecurity Improvement Act of 2020 requires government agencies to ensure the security of their IoT devices and requires NIST to develop and publish standards and guidelines for the federal government.[23] The Act follows the promulgation of guidelines and recommendations for best practices from several U.S. government agencies (e.g., NIST, FTC, DHS, GAO, NTIA, and NHTSA) and industry groups (e.g., CTIA, GSMA, and ISO).

Security of distributed Digital Twin systems pose unique challenges from a legal perspective. For example, it can be difficult to ascertain which laws apply to a distributed Digital Twin system in cyberspace that crosses jurisdictional boundaries and processes data from consumers and systems across those boundaries. Similarly, laws can be difficult to enforce across jurisdictional boundaries and in distributed Digital Twin systems where it is difficult to identify a malicious actor or device. Contractual provisions may ameliorate some of these difficulties, such as specifying choice of law, forums for dispute resolution, as well as permitted uses of a distributed Digital Twin system.

5.1.3 Compliance Strategy and Best Practices

Many countries and jurisdictions are trending towards increased privacy and data protection regulations, and non-compliance comes with tremendous financial and reputational risks. For example, non-compliance with the GDPR may result in a fine up to 20 million Euros or 4% of annual global turnover – whichever is higher. A data breach may result in a class action litigation as discussed above. In addition, as consumers demand greater protection and control over their personal information, companies can distinguish their goods and services in the marketplace based on

[22] *See* https://www.ftc.gov/news-events/events-calendar/privacycon-2020 and https://www.ftc.gov/news-events/blogs/business-blog/2021/07/get-ready-privacycon-july-27th

[23] NIST Cybersecurity for IoT program, available at https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

their privacy and data protection practices, and often face the ire of the public for mishandling of consumer data.

No one-size fits all approach exists for organizations looking to establish a compliance strategy, but there are helpful tools to get started. For example, the U.S. National Institute for Standards and Technology (NIST) has set forth a cybersecurity framework[24] and a privacy framework[25] that are broadly applicable to most organizations. The NIST cybersecurity framework is organized into five core functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. NIST organized the privacy framework into three parts: (1) Core, (2) Profiles, and (3) Implementation Tiers.

In our experience, several key considerations demonstrate that an organization has established and is practicing "reasonable" privacy and data protection measures. Entities should develop and implement a compliance strategy and framework for risk management to establish best practices for legal and regulatory compliance (Fig. 15).

A typical compliance strategy and framework encompasses, *inter alia*:

- Establishing a governance structure to define, document, communicate, and assign accountability for privacy policies and procedures.
- Understanding personal data inventory, retention, and transfer. A key foundational step in establishing a privacy compliance strategy and developing a program is understanding what data (PI) is being managed.
- Developing privacy notices applicable to each type of data subject and internal privacy policies for the organization.
- Managing requests from individuals to provide the type of PI collected, sold, or disclosed, to provide a copy of the PI, and to maintain and honor consent preferences.
- Understanding where PI is being shared with vendors, service providers, and other third parties, and establishing oversight
- Everyone who handles PI, including decision-makers, should receive training in the organization's privacy programs and policies

In addition, data protection requires an organization to implement reasonable administrative, technical, and physical security safeguards to protect covered PI/PII. An organization should define an organized approach to managing the occurrence and aftermath of a data privacy incident, security breach, or cyberattack – preferably well in advance of any potential incident (Fig. 16).

Increasing regulation – and penalties for non-compliance – are likely to favor certain implementation aspects of DT technology. Accordingly, we encourage organizations to engage in early and continuing discussions surrounding implementation of privacy and data protection measures in any new personal DT technology. For example, DT designs that use non-personalized information, or anonymized or

[24] NIST Cybersecurity Framework available at https://www.nist.gov/cyberframework

[25] NIST Privacy Framework available at https://www.nist.gov/privacy-framework

Fig. 15 Compliance strategy & framework for risk management

pseudononymized information, may be favored over DT implementations that use personalized information. Organizations may design DT technology in accordance with privacy by design and security principles at the outset. In fact, some organizations view privacy and data security controls as a competitive advantage, and such organizations distinguish their technology goods and services in the market based on their adherence to privacy and security by design. To simplify compliance, providers may restrict access and dissemination of data across different jurisdictions and entities. Additionally, DT technology providers should proceed with caution and assess any impact on individuals' privacy rights when aggregating PI/PII across different applications and use cases.

As a final note, compliance with an increasingly complex privacy and data protection regulatory and legal framework is a distinct issue from broader digital ethical questions raised by building, using, and selling new personal DT applications. At minimum, however, compliance will help ensure that an organization's practices align with consumers' expectation for security and confidentiality of their PI/PII.

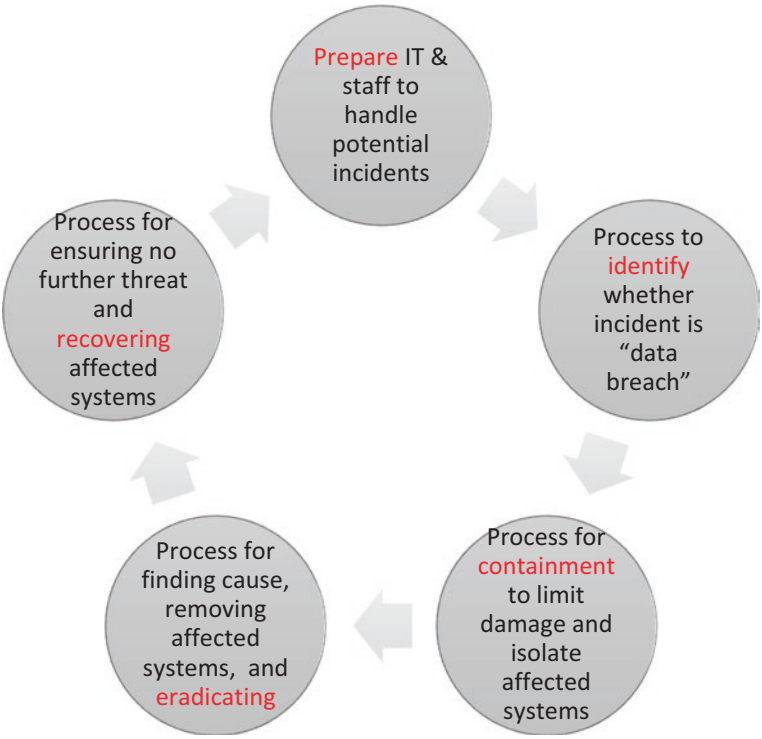

Fig. 16 Data privacy breach management plan

6 Assessing the Digital Twin Technology for Potential Bias, Trustworthiness and Transparency, and Developing a Mitigation Strategy

Many organizations use DT applications for descriptive or informative purposes, for instance, to describe the current state of a system or asset and to present diagnostic information, with a more specific example being a current health or condition indicator. More recently, DT technology that leverages large datasets and artificial intelligence (AI) and machine learning (ML) capabilities has proved capable of predicting a system's future state or performance and providing prescriptive or recommended actions based on the prediction. Yet, more advanced DT technology may soon have the capability to act autonomously without human input, *e.g.,* close the control loop such that the DT technology makes decisions and executes actions based on those decisions. For example, Digital Twin technology integrated with blockchain networks can automatically execute smart contracts at certain project milestones or on other conditions. Indeed, smart automation, interconnectivity,

decentralization, and data exchange in manufacturing technologies and processes are at the forefront of what has been coined the "Fourth Industrial Revolution."[26]

Advanced DT technology coupled with cutting edge developments in IoT, AI/ML, and other digital technologies will fundamentally alter and transform nearly every aspect of society. World leaders and regulators have taken notice and are performing the delicate task of targeting the most harmful and dangerous uses of automated technology without stifling innovation. Lawyers and prosecutors are also applying existing laws in ways that test the outer bounds of legal precedent to address novel technological harms. The following sections address regulatory oversight and legal liability associated with automated decision-making processes of advanced predictive, prescriptive, and autonomous DT technology, as well as best practices.

6.1 Regulatory Framework

As with DT technology, the United States does not have legislation broadly directed to AI-enabled automation technology. However, several states and federal agencies have formed task forces to examine AI technologies and recommend how to use and regulate such technologies. Additionally, regulators have passed laws and regulations to address certain automation technology.

Regulation of automated technology should come as no surprise in industries that are already highly regulated, such as the automobile industry. Autonomous or self-driving vehicles are subject to heightened regulation in the United States. Nevada was the first state to adopt legislation concerning the testing of autonomous vehicles in 2011, and the United States Department of Transportation developed the Automated Vehicles Comprehensive Plan to prioritize safety while preparing for the future of transportation.[27] When accidents do arise, it can be difficult to ascertain who is at fault: the passenger, the automaker, the software developer, or someone else. Additionally, technology ethicists clash as to whether the infamous Trolley Problem – the ethical dilemma of choosing to sacrifice one person to save a larger number from an accident – is applicable to how autonomous vehicles operate, and if so, how decisions should be made.

Regulators have also implemented more narrow regulations of autonomous technology. For example, facial recognition technology that law enforcement uses to automatically identify potential targets has come under intense scrutiny in the United States due to concerns of privacy erosion, reinforcement of bias against Black people, and misuse. As a result, a handful of jurisdictions have banned or

[26] Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum (Jan. 14, 2016), available at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[27] Automated Vehicles Comprehensive Plan, available at https://www.transportation.gov/av/avcp

restricted law enforcement from using facial recognition software.[28] In addition, companies and researchers are pushing back on what they view as unethical uses of facial recognition technology.[29] Remote tracking and surveillance more generally has come under scrutiny. For example, in *Carpenter v. U.S.,* 138 S. Ct. 2206 (2018), the United States Supreme Court upheld protection of privacy interests and expectations of privacy in time-stamped cell-site location information. A handful of jurisdictions have also passed legislation related to drone privacy, which prohibits the use of drones to commit video voyeurism in violation of a party's reasonable expectation of privacy.

AI/ML is also increasingly used to automate aspects of the hiring process, including recruiting, screening, and predicting the success of potential applicants. Unfortunately, studies show that several automated hiring applications promote biased hiring due to reliance on faulty data or unconsciously prejudiced selection patterns such as demography.[30] Illinois passed the Artificial Intelligence Video Interview Act (820 ILCS 42) that requires employers to disclose the use of artificial intelligence analysis of applicant-submitted videos and to obtain consent from the applicant to be evaluated by the disclosed artificial intelligence program.

Chat bots that autonomously engage with consumers have also come under scrutiny. For example, California passed the Bolstering Online Transparency (BOT) Act, which regulates online chat bots. The BOT Act prohibits certain public-facing sites or applications to use a bot to communicate or interact online with a person in California to incentivize a sale or transaction of goods or services or to influence a vote in an election without first disclosing that the communication or interaction is via a bot. The statute defines a "bot" as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person."

While similar legislation does not (yet) exist in the United States, it is important to note that Europe's GDPR already expressly provides that a data subject "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" (Art. 22).

6.2 Developing a Mitigation Strategy

As with other autonomous technology, organizations providing advanced DT technology will have to carefully consider what decisions, if any, are being made about the underlying information, and by what or whom. For example, will a human

[28] For example, Virginia and Vermont have passed outright bans applicable to law enforcement use.

[29] *See, e.g.*, Richard Van Noorden, "The Ethical questions that haunt facial-recognition research," Nature (Nov. 18, 2020), available at https://www.nature.com/articles/d41586-020-03187-3

[30] *See, e.g.*, Dawn Zapata, "New Study Finds AI-enabled Anti-Black bias in Recruiting," Thomson Reuters (Jun. 18, 2021), available at https://www.thomsonreuters.com/en-us/posts/legal/ai-enabled-anti-black-bias/

approve a proposed recommendation from a DT system, or will the DT system have control processing that can automatically implement the proposed recommendation? There are understandably several safety considerations at stake, and when something goes differently than planned, ascribing fault for the resulting harm will test the boundaries our existing legal system. For example, new fact patterns concerning autonomous systems will raise questions such as how will harm and liability be defined, what is the standard of care for an automated system, who or what is responsible when an accident occurs, does a record need to be maintained of the automated decision, how will the technology be examined in a court of law, and what are the ethical, legal, and social implications.

Accordingly, organizations making, using, and selling automated DT technology must consider the foreseeable potential harms of the technology to ensure that the technology is developed and used in safe, effective, and legally compliant manner. This consideration is especially true for technologies that affect substantial rights of individuals, such as the right to privacy and equal treatment under the law. To increase certainty, entities entering into an agreement should specify contractual liabilities and responsibilities when these foreseeable potential harms arise in the Digital Twin context. For example, an indemnity provision can specify under what conditions one party agrees to take responsibility and pay for any losses or damages caused by another party. A limitation of liability provision may excuse a party from liability under certain circumstances or place a financial cap on such a liability.

One foreseeable harm is bias in autonomous technology, which at this point is a well-documented problem. For example, developers may introduce bias into systems due to prejudiced assumptions made in algorithm development or in the training data. Indeed, several of the regulations discussed above are the result of unjustifiable racial bias present in automated systems, such as facial recognition and hiring tools. Racial bias has also arisen in healthcare risks algorithms, sentencing tools, and advertising targeting tools, among many others. Thankfully, numerous researchers, industry groups, organizations, and government are tackling the problem of how to manage bias in automated systems. NIST has also outlined a Proposal for Identifying and Managing Bias in Artificial Intelligence.[31] Organizations should stay abreast of best practices and developments to identify and manage harmful bias in automated decisions more effectively.

In our experience, trust built through transparency is of utmost importance in limiting the legal risks associated with autonomous technology. Many of the regulations discussed above address transparency, which require express, knowing, and voluntary consent from consumers before engaging with autonomous systems. As discussed in the preceding section, organizations can divulge certain details of their DT technology and systems to the discerning public without having to forfeit important intellectual property rights, such as patent rights.

[31] NIST Proposes Approach for Reducing Risk of Bias in Artificial Intelligence (June 22, 2021), available at https://www.nist.gov/news-events/news/2021/06/nist-proposes-approach-reducing-risk-bias-artificial-intelligence

7 Summary and Conclusions

Advancements in Digital Twin technology test the bounds of our legal system in many ways. A myriad of laws, rules, and regulations are worthy of consideration for any new and innovative technology, and even more so for one as broad ranging and comprehensive as the Digital Twin ecosystem. The foregoing sections describe a strategic, stepwise approach for organizations developing, implementing, deploying, and/or using large-scale complex systems like a Digital Twin. This approach includes: (1) assessing the availability and different forms of IP protection for the Digital Twin technology, (2) conducting IP due diligence search and review in connection with freedom to operate and IP clearance opinions, (3) assessing and negotiating necessary contract rights and establishing a licensing regime for the Digital Twin technology, (4) identifying and assessing compliance with applicable US and International government regulations, and (5) assessing the Digital Twin technology and, particularly, the data used and algorithms and models applied, for potential bias, trustworthiness, and transparency, and developing a mitigation strategy.

Currently, organizations may choose to seek a wide variety of IP rights for Digital Twin technology, including patent rights, trade secret rights, copyright rights, and trademark rights. These IP rights – and the legal issues and potential disputes that arise from securing and enforcing those rights – will continue to shape the expectations and decisions of investors and industry participants who seek to use or build upon Digital Twin technology for innovation. Indeed, the United States Patent and Trademark Office has noted that one "hallmark of valuable new technologies is an increase in patent applications," and such "applications reflect the expectations and decisions of investors and innovators who seek to use or build on the new technologies for innovation."[32] On the flipside, an IP due diligence search and review, often referred to as "freedom-to-operate" or clearance search, coupled with a legal opinion, will help an organization mitigate the risks of their Digital Twin technology violating the IP rights of third-parties. Moreover, organizations should assess, negotiate, and secure any necessary contract rights and establish an IP licensing and enforcement strategy for their Digital Twin technology.

Continuing advancements in virtual/augmented/mixed reality, artificial intelligence, machine/deep learning, internet of things, blockchain, biotechnology, big data and analytics, and quantum computing present new and continuing challenges from legal, regulatory, and ethical perspectives. Organizations that leverage large datasets containing personally identifying information are subject to global regulations that address the privacy rights of individuals. In addition to managing the collection, use, disclosure, retention, and distribution of individual's personally identifiable information in "personal" Digital Twin systems, organizations must ensure that those systems adequately protect such information from unauthorized

[32] "Inventing AI; Tracing the diffusion of artificial intelligence with U.S. Patents," Office of the Chief Economist in Data Highlights (Oct. 2020, United States Patent and Trademark Office), p.4, available at https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf

disclosure and use. Privacy and data protection risks only further compound when organizations use the Digital Twin as a platform for IoT technology distributed across different jurisdictions and entities. Moreover, regulators will continue to evaluate potential societal abuses of the automated decision-making processes of advanced predictive, prescriptive, and autonomous Digital Twin technology.

As a concluding remark, as Digital Twin technology continues to evolve, so too will regulations and laws that surround its use. Accordingly, organizations should implement and revisit the foregoing approach at regular intervals throughout the lifecycle of the Digital Twin technology.

Martin M. Zoltick is a technology lawyer with more than 30 years of experience representing inventors, innovators, entrepreneurs, and investors. Marty regularly works with early-stage, emerging, middle market, and mature companies, and with venture firms. For years, Marty has advised tech startups on developing IP strategies and implementing those strategies to secure IP rights, building a portfolio of IP assets, and monetizing those assets through strategic investments, licensing, enforcement, and acquisition. He is a shareholder at Rothwell Figg in Washington, DC, and is recognized as one of the World's leading patent professionals (IAM Patent 1000), an IP Star (Managing Intellectual Property), and has been selected as a Washington, DC Super Lawyer (2013–2021). Marty has a degree in computer science and, prior to attending law school, he worked for several years as a software developer. His practice is focused primarily on IP, transactions, and privacy law issues, with the majority of matters that he has handled over the past 30 years involving software technologies, including operating systems, networking, telecommunications, client/server, P2P, real-time systems, virtual networking, IOT, Big Data, AI, ML, neural networks, and quantum computing. He has developed a particular expertise with handling the legal aspects of open source software (OSS), including licensing, due diligence, compliance programs, and IP protection. He is a registered patent attorney, and a substantial part of his practice involves drafting and prosecuting patent applications. Marty also has significant experience handling contested cases and disputes on behalf of his clients. He regularly serves as trial counsel in major patent disputes in the U.S. federal district courts and as lead counsel in post-grant proceedings before the U.S. Patent and Trademark Office Patent Trial and Appeal Board. A Certified Information Privacy Professional in the United States (CIPP/US), he also helps clients understand and navigate the rapidly evolving area of privacy and data protection law. Marty is a competitive Masters swimmer and regularly competes in U.S. Masters Swimming Meets, as well as competing in open water swims in the U.S. and abroad.

Jennifer B. Maisel is an emerging thought leader on the intersection of AI and the law. Jen is a partner at Rothwell Figg in Washington, DC, and focuses on IP and privacy law issues involving cutting-edge technology. Her practice encompasses all aspects of IP law, including litigation, patent prosecution, transactions, opinions, and counselling. Jen is also a Certified Information Privacy Professional in the United States (CIPP/US) and counsels clients on privacy and data security matters. She serves a diverse range of clients – from solo inventors and start-ups to Fortune 100 companies – in matters concerning AI and machine learning, telecoms systems, the Internet of Things, Big Data technologies, blockchain, mobile and website applications, and other digital technology. She has been selected to the Washington, DC Super Lawyers 'Rising Star' list (2018–2021) and is included in the inaugural edition of Best Lawyers: Ones to Watch (2021), which recognizes extraordinary lawyers who have been in private practice for less than 10 years.