Legal 500
Country Comparative Guides 2024

United States

TMT

Contributor

Baker McKenzie LLP

Samuel G. Kramer

Partner | samuel.kramer@bakermckenzie.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in United States.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

United States: TMT

1. Is there a single regulatory regime that governs software?

No, there is no singular regulatory regime that governs software.

2. How are proprietary rights in software and associated materials protected?

Software is protected by U.S. copyright laws and international treaties. Registration of copyright is available (and required for enforcement proceedings), but copyright protection attaches from the moment the work is fixed. The source code to software, if properly maintained in confidence, may be treated as a trade secret. Software may also be eligible for patent protection; however, the patent-eligibility of software has been narrowed significantly by the courts in recent years.

The U.S. Supreme Court recognized software implemented business processes as patentable in its 1998 *State Street Bank* decision. After a decade of overly broad software patents issued by the patent office, the Supreme Court once again ruled on the patentability of software-implemented business processes in *Bilski v. Kappos* and substantially narrowed their eligibility for patent protection. Subsequently, in *Alice Corp v. CLS Bank*, the Supreme Court emphasized that embodying otherwise common aspects of business operations in software would not be eligible for patent protection.

The Federal Circuit's 2018 decision in *Berkeimer v. HP Inc.* limited patent rejections and invalidations based upon well-understood or common activities. In January 2019, the US Patent and Trademark Office issued its Revised Patent Subject Matter Eligibility Guidance memo setting out the procedures for applying subject matter eligibility criteria. Recent Federal Circuit court rulings have also narrowed patentability exclusions, making room for greater patentability of software. However, in 2022, the U.S. Supreme Court turned away two cases that offered the opportunity the further clarify the patentability of software inventions.

Software is also protected by contract under the terms of the licensor's license agreement. In *Pro CD v. Zeidenberg*, the court upheld the use of a shrinkwrap license agreement to extend the protection afforded by federal copyright laws' exclusive rights.

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

In the absence of ownership transfer under a development agreement, the person who created the software will own the proprietary rights in the software created. Software created by employees within the scope of their employment will be owned by their employer upon creation. There are also categories of works that are owned by the commissioning party in the first instance. For example, the copyright in a work made for hire, or a contribution to a collective work, vests in the commissioning party upon creation, without the requirement of a written assignment from the creator.

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There are no laws that are specific to software and computer systems with respect to the harm they may cause. Traditional legal concepts, including negligence and warranty, have been used to provide recourse to persons who have suffered damages from defective software or computer systems. Note, however, that courts may decline to extend remedies for defective goods, such as product liability principles, to software. In *Quinteros v. InnoGames*, the court held "[O]nline games are not subject to Washington's product liability law. [It] is software as a service, not an 'object,' hence Plaintiff's product liability claim must fall as a matter of law."

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 ("CFAA") criminalizes various computer-related conduct, such as intentional access to protected computers without authorization and obtaining information (18 U.S.C. § 1030(a)(2)(c)); knowing access to protected computers with intent to defraud if the value of the use exceeds $5,000 (18 U.S.C. § 1030(a)(4)); knowing transmission of programs, information, codes, or commands and thereby intentionally causing damage to protected computers (18 U.S.C. § 1030(a)(5)(A)); intentional access to protected computers without authorization and the resulting damage (18 U.S.C. § 1030(a)(5)(B-C)). The phrase "protected computer" in the CFAA refers to any computer used in interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(2)(B).

Other federal statutes, such as the Securities Act of 1933, have been amended to cover computer-related conduct, and computer-related crimes such as hacking also can be prosecuted under numerous other federal statutes, including, e.g., the Copyright Act, the National Stolen Property Act, mail and wire fraud statutes, the Electronic Communications Privacy Act of 1986, the Telecommunications Act of 1996, and the Child Pornography Prevention Act of 1996.

Finally, many states have enacted anti-hacking and/or anti-wiretapping laws designed to address computer-related crimes. State consumer fraud statutes and other state tort and contract theories (e.g., trespass, invasion of privacy) also may be used to address computer crimes such as hacking.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

There are no technology specific laws governing the provision of software between a vendor and a customer. Export control regulations may attach to specific technologies, such as those with both commercial and military application, to restrict the export, deemed export and transhipment of controlled technologies to specific countries and their nationals.

The Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") permits US law enforcement to compel U.S. technology companies to provide data requested in lawfully issued subpoenas, even if the data is stored on servers located offshore.

Certain states have enacted technology specific laws. In California, the Bolstering Online Transparency Act (BOT Act) makes it unlawful to interact with a person online to incentivize a sale or transaction in goods or to influence a vote in an election without disclosing that the communication is with a bot. In Illinois under the AI Video Interview Act, employers are required to disclose and obtain the consent of the applicant to use artificial intelligence applications in the evaluation of an applicant. Illinois' Biometric Information Privacy Act broadly requires an individual's consent to collect or disclose their biometric identifiers, with each use constituting a separate claim. Maryland enacted a statute prohibiting use of facial recognition technology to create of a facial template during pre-employment interviews without the applicant's consent.

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, software vendors typically cap their liability, subject to certain exceptions. In a perpetual license model, software vendors will typically cap their liability at the fees paid by the licensee for the software. Under term based licenses, and software as a service, vendors will frequently limit their liability at fees paid during the 12 months immediately preceding the event giving rise to the liability.

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

(a) Breaches of confidentiality are typically excluded from liability caps in software licenses and SaaS agreements. However, vendors frequently neglect to exempt these breaches from the liability exclusions concerning the non-recoverability of indirect damages, which are the type of damages that typically arise from breach of confidentiality (e.g., lost profits). (b) Data protection breaches typically are not unlimited but are frequently capped by some multiple of the ordinary liability cap (e.g., 3 to 5 times the ordinary liability cap). (c) Data security breaches are not typically addressed separately in the liability exclusions of a license or SaaS agreement; rather, a data security breach that expose personally identifiable information are treated as a data protection breach, and data security breaches that expose sensitive business information are treated as a confidentiality breach. (d) IPR infringement claims are typically limited to indemnification of third-party claims alleging infringement, and in those cases, the liability is uncapped. However, the uncapped indemnity for third party IPR claims typically have both substantive and procedural requirements, including granting the vendor sole control of the defense or settlement of the claim, and excluding claims arising from the licensee's failure to implement updates that would have eliminated the infringement. (e) Breaches of applicable law are not typically excluded from the liability limitations in software license and SaaS agreements. (f) Regulatory fines are not typically excluded from the liability limitations in software license and SaaS agreements. (g) Wilful or deliberate breaches are usually referred to as 'intentional misconduct' or intentional wrongdoing' and are typically excluded from the liability limitations in software license and SaaS agreements.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

It is not typical for a software vendor to put standard software in escrow for the benefit of a non-exclusive licensee. The source code to specially developed software, or customized software, is often placed into escrow and subject to a tripartite source code escrow agreement among the vendor, the licensee and the escrow agent, identifying the release conditions.

10. Are there any export controls that apply to software transactions?

Yes, the export of software and related technical information is subject to export controls under the Export Administration Regulations and the International Traffic in Arms regulations. Unless the software and related technical information falls under the EAR 99 "no license required" exception, the export will require a license from the Bureau of Industry and Security.

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

There are no omnibus laws that regulate outsourcing at the national or state level. There are sectoral regulations that apply to outsourcing of core services. For example, the Federal Reserve and the Office of the Comptroller of Currency and the Consumer Financial Protection Bureau all require covered institutions to maintain certain risk management standards in their agreements with third party providers of core services.

Under the pandemic related Coronavirus Aid, Relief and Economic Security Act ("CARES Act"), mid-size businesses were eligible for direct loans from the federal government. Loan recipients were required to certify that they would not outsource or offshore jobs for the term of the loan plus two years.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

There is no law or regulation in the U.S. that protects the employment of an individual in the event their job function is transferred to a third party. At the federal level, the Worker Adjustment and Retraining Notification Act ("WARN Act") requires employers with more than 100 employees to provide at least 60 days' advanced notice of planned closings and mass layoffs. State versions of the WARN Act may impose more stringent obligations, such as longer notice periods or higher damages for non-compliance.

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The term "telecommunications service" is defined by the Federal Communications Commission ("FCC") to mean the offering of telecommunications – i.e., the transmission of information of the user's choosing, without change in the form or content of the information as sent and received – for a fee directly to the public, or to such classes of users as to be effectively available directly to the public. International common carriers are required to obtain FCC authorization. In addition, most states, including California, require intrastate domestic common carriers to obtain a state authorization through public utility commissions ("PUCs").

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

The principal standard setting body for the U.S. government is the National Institute of Standards and Technology (NIST), an agency of the U.S. Commerce Department. NIST developed the Cybersecurity Framework in 2014 that is used by federal agencies to reduce cybersecurity risks. The framework is mandatory for federal agencies and is used voluntarily by many companies in the private sector. In 2022, NIST issued SP 1800-33, a draft standard for 5G cybersecurity.

The FCC is the principal telecommunications regulator in the U.S. Through its orders, the FCC mandates technical requirements for mobile operators. For example, the FCC issued an order in 2024 mandating the technical requirements for implementing the mobile challenge, verification, and crowdsourcing processes required by the Broadband DATA Act.

The Food and Drug Administration (FDA) is the principal regulator of pharmaceutical and health care products. The FDA Data Standards Catalog lists the standards supported by the FDA for use in regulatory submissions to the agency, including for connected medical devices.

The National Highway Traffic Safety Administration sets the Federal Motor Vehicle Safety Standards, and updated those standards in 2022 to address occupant protection and crash reporting with respect to autonomous vehicles.

Other standard setting bodies have promulgated technical standards in these areas, including the International Standards Organization, the Telecommunication Standardization Bureau of the ITU-T, and Underwriters Laboratories.

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards for mobile devices increase the interoperability of connected devices, a necessary feature for the growth of the Internet of Things. Standardization can avoid device manufacturers from creating proprietary technologies that are incompatible. Technical standards for connected devices allow developers to create applications that can be used on a variety of devices and networks that increase choice for consumers. It is important, however, that technical standards are not so limiting that they stifle innovation by discouraging device manufacturers from exploring new ideas and technologies.

The growth of connected devices increases risks to device and network security. Common technical standards will be an important driver in protecting connected devices from hacking and other security risks. The goal will be to institute common security standards that are not so prescriptive that they limit innovation and choice.

16. When negotiating agreements which involve mobile communications or other connected technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

Standard Essential Patents (SEPs) are those patents that read on standards that have been adopted by standard setting bodies, and would be infringed by inventions that comply with those standards. SEPs must be made available by patentees to licensees under fair, reasonable and non-discriminatory (FRAND) terms.

In 2013, the U.S. Department of Justice (DOJ) together with the US Patent and Trademark Office (USPTO) issued a joint policy statement on remedies for infringement of SEPs. Those guidelines suggested (erroneously, in the view of these agencies) that certain exclusionary remedies, including injunctive relief, should not apply to the infringement of SEPs. This presumably arose from the essential nature of SEPs that would otherwise exclude the availability of standard-compliant inventions in the marketplace if the patentee and licensee were unable to conclude a FRAND license agreement and the patentee obtained an injunction against sale of the invention. In 2019, the USPTO, DOJ and NIST issued a joint policy statement revoking the 2013 policy statement and replacing it with one that expressly acknowledges that no remedies are foreclosed in SEP infringement cases, and that the impact of exclusionary remedies is only one factor to be taken into account by the courts and agencies in assessing the appropriate remedy for SEP infringements.

In light of the new policy statement (or clarification) that all remedies remain available, when negotiating agreements that involve SEPs in mobile communications, such as patents related to 5G and WiFi 6 standards, parties need to consider the potential impact of exclusionary remedies including injunctive relief. The joint policy statement may put more pressure on SEP licensees to accept FRAND licensing terms offered by patentees because of the risk that products infringing SEPs may not be subject to damage claims alone, but may be kept out of the market entirely through injunctions or other exclusionary remedies.

17. Which body(ies), if any, is/are responsible for data protection regulation?

The Federal Trade Commission ("FTC"), under its general Section 5 authority to prevent unfair and deceptive practices, also enforces protections for personal data by requiring companies to observe the promises made by a company in its privacy policy. The FTC also enforces sectoral privacy regulations. At the state level, it is typically the state's attorney general that enforces the privacy laws and regulations enacted in their states.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The U.S. does not have omnibus protection for personal data; rather, it has taken a sectoral approach. Health related information is protected under the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA's Privacy Rule (and the privacy requirements under the Health Information Technology for Economic and Clinical Health Act ("HITECH Act")) regulate the use and disclosure of protected health information by "covered entities", such as health plans, insurers and medical service providers, as well as "business associates", such as contractors and other service providers to covered entities. Individuals have a right to know the protected health information held by a covered entity and to require the correction of inaccurate information. HIPAA's Security Rule requires covered entities and business associates to maintain administrative, physical and technical measures to protect health information.

Consumer financial data is protected under the Financial Privacy Rule pursuant to the Gramm-Leach-Bliley Act ("GLBA"). The Privacy Rule requires financial institutions to provide privacy notices to consumers that permit them to opt out of sharing financial data with unaffiliated third parties. GLBA's Security Rule requires written security procedures to be in place for the safeguarding of consumer financial information. The Fair Credit Reporting Act ("FCRA") and the Fair and Accurate Credit Transactions Act ("FACTA") regulate the use of consumer credit information, entitle consumers to a free copy of their credit report from each credit reporting agency and provide for disputing inaccurate information.

The FTC, under its general Section 5 authority to prevent unfair and deceptive practices, also enforces protections for personal data by requiring companies to observe the promises made by a company in its privacy policy.

All 50 states have enacted legislation requiring notice to customers when a security breach has or is reasonably believed to have exposed a consumer's personal information. Personal information under data breach is typically defined as a first name or initial, a last name, plus a social security number, driver's license or state ID number or an account number with a password or PIN. Recently, states have expanded this definition to include login credentials plus password. Recently, some states have begun to include biometric information as personal data for purposes of breach notification laws. The threshold for notice, timing requirements and liability vary by state.

The California Consumer Privacy Act of 2018 ("CCPA") came into effect in 2020, and requires all businesses dealing with California residents to observe restrictions on data monetization, accommodate individuals' rights to access, deletion, and transfer of personal data of California residents and households. The California Privacy Rights Act ("CPRA") was adopted by ballot initiative in 2020 and came into effect January 1, 2023. The CPRA creates a right to opt-out of sharing of personal information and certain uses of sensitive personal information, a right to correct inaccurate personal information and new rights with respect to business's personal data practices and use of automated decision-making technologies. The CPRA creates a new state agency, the California Privacy Protection Agency, that assumes all rulemaking and enforcement authority previously vested in the California attorney general.

Other states have adopted data privacy protections for consumers in their states, including the Virginia Consumer Data Protection Act (effective January 1, 2023), the Colorado Privacy Act (effective July 1, 2023), the Utah Consumer Privacy Act (effective December 31, 2023), the Connecticut Data Privacy Act (effective July 1, 2023), the Iowa Data Privacy Law (effective January 1, 2025), Indiana Data Privacy Law (effective January 1, 2026), Tennessee Information Protection Act (effective July 1, 2025), Montana Consumer Data Privacy Act (effective October 1, 2024), Texas Data Privacy and Security Act (effective July 1, 2024), Delaware January 1, 2025), Florida Digital Bill of Rights July 1, 2024), Oregon

Consumer Privacy Act (effective July 1, 2024), New Jersey Data Privacy Law (effective January 15, 2025), Kentucky Data Privacy Law (effective January 1, 2026), Nebraska Data Privacy Act (effective January 1, 2025), New Hampshire Privacy Act (effective January 1, 2025), Maryland Online Data Privacy Act (effective October 1, 2025), Minnesota Consumer Data Privacy Act (effective July 31, 2025), and the Rhode Island Data Transparency and Privacy Act (effective January 1, 2026).

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Typically, violations of data protection laws permit recovery of actual or statutory damages and attorneys' fees. Privacy violations under the FTC Act have a maximum fine of $16,000 per violation. Civil violations of HIPAA have a maximum fine of $1.5 Million. The maximum civil fine for GLBA violations is $1 Million. Under the CCPA, the California attorney general can impose fines of $2,500 for non-willful violations and up to $7,500 fines for willful violations, with a private right of action for individuals whose information is accessed or disclosed as a result of a breach of a business' duty to maintain reasonable security. The CPRA adds fines of up to $7,500 for violations (even if unintentional) of the consumer privacy rights of minors.

The VCDPA and UCPA provides for fines of up to $7,500 and the CDPA provides for fines of up to $5,000, in each case for willful violations of the law. While not having a specific statutory fine for non-compliance, the Colorado Privacy Act, by reference to CPA violations constituting a breach of the Colorado Consumer Protection Act, includes fines of up to $20,000 per violation.

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Technology contracts frequently involve the cross border collection and processing of personal data, and in such cases, they will refer to GDPR. Where contracts have the potential to involve the collection of personal data on California residents or households, the contract will refer to CCPA and CCPR. Occasionally, contracts without a clear international element may refer to GDPR for principles of how personal data is collected and processed, even in cases where no data of individuals in the EU is implicated.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

There is no body that is specifically charged with regulating artificial intelligence ("AI") in the U.S. Federal agencies are issuing guidance in connection with the use of AI. The FTC issued guidance to businesses on unlawful discrimination due to bias in AI algorithms as well as a warning to marketers about exaggerating the results that AI powered products can deliver. The Food and Drug Administration ("FDA") has issued guidance that some AI tools should be regulated as medical devices under the FDA's oversight of clinical decision support software.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The National Artificial Intelligence Initiative Act of 2020 ("NAIIA") directs the President of the United States to support AI research and development, education and worker training, coordinate interagency AI activities and work with strategic allies on development of trustworthy AI systems.

In 2022, the White House released a policy paper entitled "Blueprint for an AI Bill of Rights", setting out policy principles for regulation of artificial intelligence.

The following is a list of some of the proposed AI legislation:

- Algorithmic Justice and Online Platform Transparency Act. Bills H.R.3611, S.1896. Seeks to prevent discrimination by algorithmic processes and increase algorithmic transparency.
- Algorithmic Accountability Act (Apr 2019). Bills S 1108, HR 2231 (Apr. 2019) intended to require "companies to regularly evaluate their tools for accuracy, fairness, bias, and discrimination."
- Facial Recognition and Biometric Technology Moratorium Act of 2021. Bill S.2052. Requires Federal agencies or officials to receive legislative approval to use biometric surveillance systems or information derived therefrom.
- Mind Your Own Business Act of 2021. Bill S.1444. Seeks to prevent algorithmic bias in high-risk information systems and automated-decision systems, and enables consumers to opt out of tracking by covered entities.
- Filter Bubble Transparency Act. Bill S.2024. Requires

online platform operators that use algorithms to customize what users see to allow users to opt out of the use of those algorithms.

Some states have enacted laws related to artificial intelligence:

- Alabama enacted a law related to elections that criminalizes distribution of materially deceptive media to influence an election.
- Colorado passed a law requiring developers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination.
- Florida enacted legislation that requires election advertisements to include disclaimers when AI is used in the ad content.
- Indiana passed a law to expand the definition of "intimate images" to include AI simulations for purposes of its sexual abuse statutes.
- Oregon updated its election law to require campaign communications that contain any synthetic media to include a disclosure that the content has been manipulated.
- Utah revised its criminal code so that judges may not rely solely on AI pretrial risk assessment tools in making any determination regarding probation.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

There is no enacted or pending federal legislation aimed specifically at generative AI or Large Language Models, rather than AI more broadly.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

There are no statutorily required provisions for technology contracts to address the risks of artificial intelligence. Best practices are starting to emerge to address use of training data and data privacy risks, ownership of the outputs of AI systems that use customer inputs, confidentiality restrictions on input data, inaccurate output of AI systems, and bias in AI models.

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Software and technology contracts frequently contain provisions that address intellectual property ownership and license rights with respect to the outputs of AI systems. Some content creators are using their copyright ownership in works to prohibit their use for training AI models.

26. What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

(i) The U.S. does not regulate blockchain technology *per se* at the federal level. Various states have enacted legislation to promote or otherwise permit the use of blockchain technology. Arizona's Electronics Transactions Act specifically recognizes electronic signatures secured on a blockchain, records and contracts secured on a blockchain and smart contracts as valid and enforceable. Delaware's General Corporation Law was amended to allow Delaware corporations to put stock ledgers on a blockchain. Vermont enacted a law which enabled blockchain records to be deemed self-authenticating under Vermont's Rules of Evidence. Wyoming amended its version of the Uniform Commercial Code to specifically define and classify blockchain secured digital assets, and to set forth the specific requirements for the perfection of a security interest in digital assets through control.

(ii) Securities: Offering securities, including certain tokens arising out of initial coin offerings ("ICOs"), triggers a requirement to register the securities with the Securities and Exchange Commission ("SEC"). With respect to ICOs, the SEC has found that certain tokens arising out of ICOs constitute securities offerings, but the SEC has also determined that bitcoin and ether are not or are no longer securities for purposes of federal securities law.

Under Section 2(a)(1) of the Securities Act and Section 3(a)(10) of the Exchange Act, the definition of security does not specify a token or coin, but does specify an "investment contract." The term "investment contract" is the residual category in the definition that captures securities that do not fall within other categories.

In *SEC v. W.J. Howey Co.*, the U.S. Supreme Court articulated a test for determining whether something is an "investment contract." The test—which has become known as the "*Howey* test"—provides that an "investment contract" is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. According to the SEC, this definition embodies a "flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits." In considering whether something is a security, "the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto."

The prongs of an investment contract, as articulated in *Howey*, are thus fourfold: (i) an investment of money (ii) in a common enterprise (ii) with a reasonable expectation of profits (iv) to be derived from the entrepreneurial or managerial efforts of others.

Prior to July, 2017, the SEC had not applied the *Howey* test to an ICO. However, on July 25, 2017, the SEC provided important initial guidance on its application of the *Howey* test to ICOs when it released a Section 21(a) Report of Investigation on its findings regarding the token sale by The DAO. The DAO functions as a decentralized autonomous organization, which essentially means a virtual organization embodied in computer code and executed on a distributed ledger or blockchain.

In its analysis of whether The DAO had improperly offered and sold securities via an ICO, the SEC noted that new technologies do not remove conduct from the purview of U.S. federal securities laws. Based on the facts and circumstances regarding The DAO's offering of tokens, the SEC found that (i) DAO tokens are securities under federal securities law, (ii) The DAO was required to register the offer and sale of DAO tokens under the Securities Act absent a valid exemption, and (iii) any exchange on which DAO tokens were traded was required to register under the Securities Act as a national securities exchange or operate pursuant to an exemption. In its report, the SEC did not say that all tokens would be securities. Rather, the SEC noted that the determination depends on the particular facts and circumstances and economic realities of the transaction.

On April 3, 2019, the SEC staff released its "Framework for 'Investment Contract' Analysis of Digital Assets" ("Framework") to provide guidance with respect to the SEC's jurisdiction over digital assets that qualify as investment contracts under the *Howey* analysis. In the Framework, the SEC did not set out specific guidelines for when ICOs are (or are not) securities, the Staff did provide a long list of considerations. Many of the considerations set out in the Framework for when an ICO would tend to be viewed as a security are, as a practical matter, present in many ICOs. This means that many ICO offerings will need to register as securities or demonstrate their exemption from registration.

On July 13, 2023, the Federal District Court for the Southern District of New York ruled that sales by Ripple of the XRP cryptocurrency to institutional investors constituted the sale of unregistered securities, but that programmatic aftermarket sales of XRP to retail investors were not sales of a security.

(ii) Commodities: Brokering transactions in futures contracts, options on futures contracts, swaps, or retail off-exchange forex contracts (collectively, "Commodity Interests") triggers a requirement to register as an introducing broker or futures commission merchant with the Commodity Futures Trading Commission ("CFTC"). Advising persons with respect to Commodity Interest transactions triggers a requirement to register as a commodity trading advisor ("CTA") with the CFTC. A CTA is an individual or organization that, for compensation or profit, advises others, directly or indirectly, as to the value of or the advisability of trading futures in commodity interests.

The CFTC has treated bitcoin as a commodity since its September 17, 2015 order against Coinflip, Inc. (doing business as Derivabit). The CFTC said it regulates bitcoin and other virtual currency derivatives just as it regulates other commodity derivatives. Coinflip, Inc. was the operator of the Derivabit platform, which marketed bitcoin put and call options. The CFTC's order did not impose any specific standards or restrictions on cryptocurrencies themselves but on derivatives that have values that are based on or reference the values of cryptocurrency. The order also triggers reporting and recordkeeping implications, minimum margin requirements and the requirement to register as a swap execution facility ("SEF") for companies that fall under that category.

In May 2018, the CFTC staff issued guidance that reiterated its position that "bitcoin and other virtual currencies are properly defined as commodities." In *CFTC v. McDonnell*, the Federal District Court for the Eastern District of New York said that "virtual currency may be regulated by the CFTC as a commodity." The CFTC's "broad statutory authority… and regulatory authority… extend to fraud or manipulation in the virtual currency derivatives market and its underlying spot market."

(iii) Money Transmission: At the federal level, companies that engage in money transmission are considered money services businesses ("MSBs"), which are regulated entities for anti-money laundering ("AML") purposes under the Bank Secrecy Act of 1970 (the "BSA"). MSBs are required to register with the Financial Crime Enforcement Network ("FinCEN") and meet other regulatory requirements, such as implementing an AML compliance program.

Under the BSA, money transmission is defined as the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.

At the state level, money transmitters are required to have licenses for each state in which they operate. Many states have expanded the definition of money transmitter to include the transmission of cryptocurrency, while others exclude cryptocurrencies from money transmitter licensing requirements. It is a federal crime to operate as a money transmitter without a relevant state license.

In 2022, the Uniform Law Commission proposed amendments to the Uniform Commercial Code, creating a new Article 12 for Controllable Electronic Records (CERs). This new Article 12 sets out rules for the perfection of security interests in CERs through control rather than possession. This addition greatly simplifies the process for establishing security interests in digital assets, including those registered on a blockchain. As of this writing, thirteen states plus the District of Columbia have adopted UCC Article 12. Fifteen states have legislation pending to adopt Article 12.

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

In 2015, the FCC adopted net neutrality principles that would require Internet Service Providers to treat all data traffic the same and not prioritize, block, slow down or charge money for specific content. In 2018, these net neutrality principles were rolled back.

The Ninth Circuit Court of Appeals in *Gonzalez v. Google*, a case alleging Google violated the Anti-Terrorism Act by "recommending" ISIS videos to users found that the claims fell within the immunity provisions of Section 230 of the Telecommunications Act. The Court held that a search engine's use of content-neutral algorithms does not create liability for serving content posted by a third party. In *Twitter v. Taamneh*, the Supreme Court held that surviving family members' claims against Twitter were not allowed under the Ant-Terrorism Act and did not address the immunity provisions of Section 230 of the Telecommunications Act. The Supreme Court remanded the *Google v. Gonzalez* case to the lower court for reconsideration in light of the *Twitter* ruling.

The FTC's .Com Disclosures guidelines sets out the requirements for online disclosures in advertising. Disclosures must be clear and conspicuous and should be placed as close as possible to the text triggering the claim. Where there are space limitations, disclosures may be made on a page linked to the ad. Such links must be obvious and appropriately labelled to indicate the nature and importance of the linked information; disclosures should not be relegated to linked terms of use. Advertisers must monitor click-through rates to gauge the effectiveness of the link.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

Section 230 of the Telecommunications Act provides that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This immunity provision means that websites, including social media sites that host content from third parties, are not responsible for screening the content posted by their users.

The FTC Endorsement Guidelines were updated to require social media influencers to disclose their relationship to company whose products or services are being endorsed, including whether the company provided them with free products, services, payments or other benefits. The updated Endorsement Guidelines expand the definition of endorsement to include verbal statements, tags in social media posts, demonstrations, depictions of the name, signature, likeness or other identifying personal characteristics of an individual, and the name or seal of an organization. The FTC also proposed a new *Rule on the Use of Consumer Reviews and Testimonials* that prohibits fake consumer reviews, materially misrepresenting a reviewer's experience with a product, service or business, including the repurposing of a review for a different product, or compensation to a reviewer conditioned on the expression of a particular sentiment (either positive or negative) regarding a product, service or business.

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

1) A federal omnibus data privacy law will be enacted to harmonize the growing number of state privacy statutes.

2) Courts will clarify the rights of providers and users of artificial intelligence to use and retention of input data for model training.

3) The authority of the SEC to regulate cryptocurrencies through enforcement will be significantly limited.

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Technology contracts do not commonly include express provisions to address sustainability and net zero commitments. However, managed service agreements typically require suppliers to comply with companies' supplier codes of conduct. Those codes of conduct will often include zero waste, greenhouse gas emission disclosures or other ESG related obligations that are designed to enable the company to meet its stated environmental goals.

Contributors

Samuel G. Kramer
Partner

samuel.kramer@bakermckenzie.com