2

Technology Trends

Wolters Kluwer | BAKER BOTTS

Technology Trends Introduction

The technology that impacts Big Data progresses at an incredible pace, and while Big Data technology has been used to solve a wide array of problems in a range of different fields, common trends can be seen even between disparate markets. Technology marches ahead, while the current legal doctrine and regulators are forced to adapt. This chapter aims to provide background on various business and legal concerns that have arisen in the Big Data industry, as well as insight into how current legal and regulatory frameworks may be applied to the challenges posed by Big Data. The chapter focuses on technologies that have garnered the attention of commentators and the public at large, such as blockchain, artificial intelligence, and biometric data.

First, blockchain technology is discussed, along with industry trends, and potential new applications of the technology, such as maintaining detailed title chains for IP assets to facilitate IP transactions. The regulatory environment and privacy concerns unique to the technology are also explored.

This chapter next addresses the current IP legal framework and its application to AI systems and the innovations made possible by AI systems. AI data privacy concerns, ethical considerations, and the ways in which AI systems are impacting the consumer and transportation sectors are further addressed. As with blockchain, the nascent regulatory environment is also examined.

Finally, the chapter concludes with a discussion of the commercial use of biometric data and the associated privacy concerns. The early stages of the regulatory framework are also explored.

Blockchain

In 2008, Satoshi Nakamoto (who has not yet been identified, but who some speculate may be a group of individuals operating under a pseudonym) released a whitepaper on a peer-to-peer digital currency system called Bitcoin.[1] This whitepaper described the use of a new technology called blockchain, which, in Nakamoto's proposal, was to be used primarily to facilitate Bitcoin transactions.[2] The utility of blockchain technology itself now extends far beyond the transfer of currency, however, due to the technology's ability to efficiently and reliably store and exchange information. As just some examples, blockchain provides new avenues for the storage and management of various types of data, such as intellectual property registrations, financial records, and digital signatures, and allows for the use of autonomously executed smart contracts.

BLOCKCHAIN TECHNOLOGY

At its core, by combining certain aspects of cryptography, decentralized consensus mechanisms, peer-to-peer networks, and distributed storage, blockchain technology reduces the role of and need for a central authority in a distributed transaction system. A blockchain is in essence a continually growing database that is distributed among certain participants in a networked system, called nodes. It is comprised of a chain of information-containing blocks, each of which also includes a timestamp, a reference to the immediately preceding block in the chain (and thereby, all the blocks before it), and a way for the nodes to validate a new block before it is added to the chain.[3] The blockchain is not stored on a single, centralized server; instead, copies of the blockchain are replicated and maintained by each of the nodes themselves, spread throughout the network.

A key component of a blockchain is the dichotomy in the level of difficulty required to make changes to its state: It is simple to add data to a blockchain, but far more difficult to remove or change data once it has been added. When a user wants to add information to the blockchain (a common form of which is a transaction between two peers), this information is broadcasted to the entire network of participating nodes,[4] who then bundle the information into a new block. However, for any node to add this new block of compiled information to the blockchain, a majority of the remaining nodes must agree—i.e., they must validate the block by way of a

[1] Satoshi Nakomoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (2009), https://bitcoin.org/bitcoin.pdf.

[2] *Id*.

[3] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* 6-7 (Mar. 12, 2015), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

[4] These nodes can generally be thought of as a network of computers, i.e., a peer-to-peer network, each running certain software that sets out the respective blockchain's protocol. In a proof-of-work system, these nodes are referred to as miners.

consensus mechanism, the most common of which is called proof of work.[5] In a proof of work system, the participating nodes compete to solve a complex mathematical problem (requiring substantial computational resources) that will allow the nodes to add a new block.[6] The first node to solve that problem broadcasts the solution to the remaining nodes, who confirm the block's validity against their own respective copies of the blockchain. When its validity is confirmed, the block is added to the chain and the victorious node is rewarded for its efforts.[7] Once a block is added to the blockchain, it can no longer be revised or deleted; it assumes its position as part of an immutable database, accessible and verifiable by all participants.[8]

SMART CONTRACTS

As a database maintained by a peer-to-peer network of computers, a blockchain enables the creation of what are known as "smart contracts." Smart contracts may be thought of as computer-coded contracts stored within a blockchain that are autonomously executed in a decentralized way upon the occurrence of some predetermined criteria.[9] That is, each of the participating nodes can, without the need for human involvement, read the smart contract and its conditions, verify its validity, and enforce its performance.[10] Degrees of objectivity and flexibility can also be implanted into smart contracts by way of an "oracle," a trusted external source used to provide extrinsic information to the smart contract.[11] As an example, where human decision making is required to determine certain terms of a smart contract, an oracle comprised of an arbitration panel or judge, or even the parties themselves, may be used.

As the use of smart contracts increases, lawyers will surely be tasked with reconciling certain aspects of classic contract doctrine with its application to smart contracts. As one example, for a typical contract to be enforceable, it must meet certain requirements, such as mutual assent,[12] consideration,[13] and capacity of the contracting parties.[14] Some contracts, such as those entered into by one party under duress or undue influence, may be voidable.[15] Given the self-executing and immutable nature of smart contracts, however, the performance of even a "voidable" smart contract might continue against the will of a contracting party.

---

[5] Proof of stake is another popular consensus mechanism that relies on the nodes staking a certain amount of value to an assertion that their block is valid. *See Proof of Stake*, Bitcoin Foundation Wiki (last edited Oct. 10, 2015), https://en.bitcoin.it/wiki/Proof_of_Stake.

[6] *See, e.g.*, Nakomoto, *supra* note 1, at 3; Vitalik Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*, Github, https://github.com/ethereum/wiki/wiki/White-Paper (last edited Sept. 15, 2017).

[7] *See* Nakamoto, *supra* note 1, at 3; *see also* Buterin, *supra* note 6.

[8] *See* Wright & De Filippi, *supra* note 3, at 8.

[9] *See, e.g.*, John Stark, *Making Sense of Blockchain Smart Contracts*, Coindesk (June 4, 2016), http://www.coindesk.com/making-sense-smart-contracts; *see also* Wright & De Filippi, *supra* note 3, at 10-11.

[10] *Id.*

[11] Shawn S. Amuial et al., The Blockchain: A Guide for Legal & Business Professionals § 2:5 (2016).

[12] Restatement (Second) of Contracts § 3 (Am. Law Inst. 1981).

[13] *Id.* § 17.

[14] *Id.* § 12.

[15] *Id.* §§ 174, 177.

If the past is any indication of the future, existing contract doctrine may simply be adapted to apply to smart contracts, as has happened in connection with other electronic agreements. For example, courts in the U.S. analyzing mutual assent (which traditionally must be manifested either orally or through writing)[16] with regard to agreements entered into online typically look for another form of affirmative action to show a party's agreement to a contract's terms, such as clicking on a button or notice.[17] Further, the Electronic Signatures in Global and National Commerce Act ("E-SIGN Act") prohibits courts from denying enforcement of electronic signatures and contracts solely on the basis of their electronic form.[18] Most states have also adopted the Uniform Electronic Transactions Act ("UETA"), which governs electronic records and signatures not covered under the Uniform Commercial Code and is intended to harmonize enforcement of electronic agreements with non-electronic agreements.[19] As such, it may be helpful to consider judicial opinions and legislation of this type for guidance when drafting and analyzing smart contracts.

POTENTIAL USES OF BLOCKCHAIN TECHNOLOGY AND INTELLECTUAL PROPERTY IMPACT

Oft-mentioned use cases of blockchain technology are financial in nature, such as the use of a blockchain to automate syndicate formation, issue private securities or shares of a company, make cross-border transactions, or enter into loan agreements.[20] Indeed, the most well-known use of blockchain technology is to allow people to buy and sell "cryptocurrencies," such as bitcoin. Other uses, including one that has gained in name recognition, is the use of the Ethereum blockchain to raise capital through what is known as Initial Coin Offerings ("ICOs"). ICOs are used by companies to offer a share value tied to the company that can be redeemed based on the company's performance and traded on a virtual platform, such as Kraken, Bittrex, and Poloniex. The boom in cryptocurrencies and the amount of money raised through ICOs have garnered much attention, and the U.S. Securities and Exchange Commission recently issued guidance on these issues, further addressed below.

In the intellectual property realm, the technology's most obvious implementation is its most basic function—a distributed database of time-stamped information—to record chain-of-title and ownership of IP assets.[21] The sequence of ownership, from inception, to registration, to initial assignment and any subsequent assignments, can be continually updated in real-time within a blockchain, creating an immutable audit trail for the transfer of any IP asset without the need to rely on a trusted third party. And with the potential for blockchain interoperability also comes the potential for a global intellectual property registry system, which could radically simplify the process of recording the transfer of intellectual property between citizens of different nations. Much of this, however, relies first on the reception of governmental agencies to adopting blockchain technology for such functions; and second

---

[16] *Id*. § 19.

[17] *See, e.g., Nguyen v. Barnes & Noble, Inc*., 763 F.3d 1171, 1175 (9th Cir. 2014).

[18] 15 U.S.C. § 7001.

[19] *Id*. § 7002.

[20] World Econ. Forum, The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services 41-44 (2016), *available at* http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

[21] *See, e.g.*, Thomas H. Vidal, *Harnessing Blockchain to Manage IP Assets*, Inside Counsel (Mar. 20, 2017) http://www.insidecounsel.com/2017/03/20/harnessing-blockchain-to-manage-ip-assets.

on the adaptation of intellectual property law to recognize blockchain registration as legitimate way to verify ownership or authorship.

IP-ownership recordation on a blockchain can be combined with other aspects of the technology to create a variety of additional use cases. Blockchain technology allows for the representation of assets in a digital form, which in turn simplifies and makes feasible the transfer of micropayments (that is, payments on the scale of pennies).[22] This brings to light a whole new paradigm for the payment of owners of creative works. As an example, the owners of the respective copyrighted works making up an online article (such as pictures or videos) could record their ownership of these works on a blockchain. A smart contract stored within that same blockchain could then be used to effectuate an internet user's automatic transmission, directly to the respective copyright owners, of very small payments in return for the consumption of their creative works.[23] The amount of such payment may be based on, for instance, the amount of time spent on the webpage hosting the article, the number of views of the article, or other metrics, all of which could be fully automated within the smart contracts.

Additionally, just as smart contracts can allow for the automatic transfer of title to assets upon the occurrence of certain events, they similarly can automatically execute and enforce the conditions (*e.g.*, territorial or temporal limitations) of licenses to IP assets. For example, imagine companies A and B agree to a patent license, wherein company A will receive a set percentage "X" of every sale of a certain item "Y" made by company B within the United States for the next three years. The parties to such a license could code and store to a blockchain a self-executing smart contract that includes all of these terms: for every item Y that is delivered to a customer within the U.S., the agreed-upon percentage X could then be automatically transferred from the value stored in company B's blockchain address to company A's blockchain address, with the smart contract's self-execution automatically stopping in three years per the terms of the code. Such a system would eliminate the need for a deposit or escrow, thereby removing the need for trust in a third party.

Finally, at least one group has proposed to use blockchain to improve innovation and prior art searching.[24] Specifically, Loci has proposed using blockchain to better track patent applications, IP development, and prior art in particular fields. Although this approach is still relatively untested, this proposal and similar ideas are another example of the potential uses of blockchain in connection with IP and broader legal issues.

REGULATORY GUIDANCE AND ADOPTION

For the early part of its existence, blockchain technology remained relatively regulation-free.[25] In recent years, however, regulators have made serious attempts to control the emerging technology, such as by releasing reports

---

[22] AMUIAL ET AL., *supra* note 11 § 7:4.

[23] *Aaron Wright on Blockchain Technology and the Law* [podcast], ALGOCRACY AND THE TRANSHUMANIST PROJECT (Nov. 4, 2016), https://algocracy.wordpress.com/2016/11/04/episode-14-aaron-wright-on-blockchain-technology-and-the-law/.

[24] *Thinking better. Together.,* Loci (last visited Oct. 31, 2017), https://locipro.com/.

[25] Carlo R.W. De Meijer, *Blockchain Regulation in the Securities Industry: still many unanswered Questions!*, FINEXTRA (Mar. 13, 2017), https://www.finextra.com/blogposting/13817/blockchain-regulation-in-the-securities-industry-still-many-unanswered-questions.

compiling the challenges created by using blockchain technology in an industry.[26] Although most of these reports are open-ended and intended to solicit further investigation and questioning, there is a clear indication that more concrete regulation should be expected in the near future. Below are some of the more prominent examples of regulatory organizations that have recently issued guidance in this area. Notably, most of these regulatory opinions discuss distributed ledger technology ("DLT") as a whole, of which blockchain is a specific type.

U.S. FEDERAL RESERVE

In December 2016, the U.S. Federal Reserve released a report called *Distributed ledger technology in payments, clearing, and settlement*.[27] The report suggests the usefulness of DLT to record asset ownership. It also covers some of the challenges regarding such use of DLT. The report, however, says little about what actions the Federal Reserve plans to take.[28]

U.S. FINANCIAL INDUSTRY REGULATORY AUTHORITY ("FINRA")

In January 2017, FINRA released a report called *Distributed Ledger Technology Implications for the Securities Industry*.[29] The report, while giving an overview of DLT, focuses primarily on how DLT may impact current securities regulations. It covers a wide range of considerations, including network security, data privacy, surveillance, and governance, but explicitly states that it is meant to be an "initial contribution to an ongoing dialogue with market participants."[30]

EUROPEAN SECURITIES AND MARKETS AUTHORITY ("ESMA")

In February 2016, the ESMA published a report called *The Distributed Ledger Technology Applied to Securities Markets*.[31] The ESMA stated that it will continue to monitor DLT and decide whether additional regulations are necessary in relation to existing EU regulations. Notably, it concluded that regulatory action as of this point is premature, but may be necessary in the long term.[32]

U.S. SECURITIES AND EXCHANGE COMMISSION ("SEC")

In July 2017, the SEC issued guidance on the ICO market. In particular, the SEC addressed the concept of whether these token offerings are subject to securities regulations, and the agency also flagged the risks associated with ICOs.[33] Although not going so far as to declare all coins associated with ICOs as securities, the SEC did conclude that U.S. securities laws apply even if a decentralized autonomous organization offers such securities and

---

[26] Peter Chawaga, *How Will Finance Approach the Regulation of Blockchain*, Nasdaq (Apr. 4, 2017) http://www.nasdaq.com/article/how-will-finance-approach-the-regulation-of-blockchain-cm769389.

[27] Fed. Reserve Bd., *Distributed Ledger Technology in Payments, Clearing, and Settlement*, 2016-095 (Dec. 5, 2016).

[28] *Id*.

[29] U.S. Fin. Indus. Reg. Auth., *Distributed Ledger Technology Implications for the Securities Industry* (Jan. 2017).

[30] *Id*.

[31] European Sec. and Markets Auth., *The Distributed Ledger Technology Applied to Securities Markets* (Feb. 2016).

[32] *Id*.

[33] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017) ("SEC Report"), *available at* https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings.

regardless of whether a virtual currency is used for the purchase.[34] With regard to the subject company of its report, DAO, the SEC concluded the tokens offered during the company's ICO, DAO Tokens, were securities and therefore subject to mandates set out in Section 5 of the Securities Act, including the filing of a registration statement.[35] The SEC limited its analysis to the particular DAO Token, but the comments are instructive of how the SEC will subject cryptographic tokens to such scrutiny.

After finding the DAO Tokens were securities, the SEC went on to conclude that a number of web-based platforms that facilitated the secondary trading of DAO Tokens "appear to have satisfied" the criteria necessitating SEC regulation pursuant to Sections 5 and 6 of the Exchange Act, and did not operate pursuant to an appropriate exemption.[36] The report does not opine on whether The DAO qualified as an investment company under Section 3(a) of the Investment Company Act of 1940, but these ramifications and applications should be considered before structuring any coin offering.

More recently, in December 2017, the SEC issued a statement on cryptocurrencies and ICOs, in which the SEC chairman warned investors of the risks inherent in these markets and financial vehicles, and indicated that he has asked the SEC's Division of Enforcement to continue to police this area vigorously and recommend enforcement actions against those that conduct initial coin offerings in violation of the federal securities laws.[37] That was followed by a January 2018 letter to representatives of the Investment Company Institute (ICI) and the Securities Industry and Financial Markets Association (SIFMA), raising similar concerns regarding investor protection, compliance issues, and market manipulation, among other issues.[38]

Some U.S. states have taken affirmative steps in adopting blockchain technology, such as Delaware's approval of legislation to use blockchain technology for state archival records and corporate recordkeeping.[39] Other states, such as Arizona and Illinois, have followed suit in welcoming the technology.[40]

Outside the U.S., some countries have endorsed the technology in other ways, such as Japan's official approval of 11 different secondary exchanges—granting them full licenses to sell cryptocurrencies like bitcoin, ether, and other

---

[34] *See id.* at 18.

[35] *See id.* at 11-15 (analyzing the DAO Token under the test promulgated in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946)).

[36] *Id.* at 16-17. Not surprisingly, companies are already looking to capitalize on the Report's guidance in this regard, such as with the September 2017 announcement of the first SEC-compliant alternative trading system for the exchange of tokens categorized in the U.S. as securities. *See, e.g.*, Ash Bennington, *Regulated ICOs Arrive: Overstock to Open Exchange for Legal Token Trading*, COINDESK (Sept. 27, 2017), https://www.coindesk.com/regulated-icos-arrive-overstock-open-exchange-legal-token-trading/.

[37] https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

[38] *See* "SEC Staff Issues Guidance on Cryptocurrency-related Holdings," THE NATIONAL LAW REVIEW (FEB. 17, 2018), https://www.natlawreview.com/article/sec-staff-issues-guidance-cryptocurrency-related-holdings.

[39] S.B. 69, 149th Gen. Assemb. (Del. 2017) (amending various sections of the Delaware General Corporation Law (DGCL)).

[40] *See* ARIZ. REV. STAT. ANN. § 44-7003 (2017) (amended by H.B. 2417) (allowing signatures "secured through a blockchain" to be considered as "electronic signatures"); H.J.R. 0025, 100th Gen. Assemb. (Ill. 2017) (creating "Distributed Ledger Task Force" to study the benefits of "a transition to a blockchain based system for recordkeeping and service delivery").

coins on the secondary market.[41] On the other hand, some countries, such as China and South Korea, have altogether banned Initial Coin Offerings.[42] China has been extreme in its measures; the government has shut down cryptocurrency exchanges, which facilitate the trading of such securities inside its borders.[43] In Singapore, the Monetary Authority of Singapore issued guidance and cautionary advice that such offerings may be subject to regulation and must follow existing laws in the country.[44]

PRIVACY RIGHTS

While the immutable nature of blockchain provides secure and trustworthy data, the technology raises privacy concerns with its ability to facilitate the storage and accessibility of sensitive data. Traditionally, individuals looking to prevent continued accessibility of such data could pursue, e.g., judicial recourse, such as injunctive relief, to halt ongoing harm. However, recourse that traditionally may be utilized to censor or redact data may prove futile in the blockchain space, because the data is immutable and, by the very nature of the technology, cannot be modified or deleted. As an example, Twister is a peer-to-peer microblogging network similar to Twitter, but uses blockchain technology.[45] The network's completely decentralized construction makes it resistant to government censorship and shutdown attempts, as there is no centralized server to target.[46]

Another area of concern involves the identification of parties involved in any blockchain-recorded transaction, such as those performed on the Bitcoin blockchain, as these transactions become more common in day-to-day activities. Although identities are psuedo-anonymous on the Bitcoin blockchain, in that addresses are not tied to the identity of users on a protocol level, it is conceivably possible to aggregate other data and patterns to tie a certain address or addresses to an individual's identity, thereby also revealing his or her spending habits.[47]

In the U.S., a variety of federal statutes address data privacy in some fashion. The application of these statutes to blockchain technology will, at some point, need to be determined. As such, companies utilizing blockchain

---

[41] *See* Takahiko Wada & Hideyuki Sano, *Japan's FSA gives official endorsement to 11 cryptocurrency exchanges*, REUTERS (Sept. 29, 2017), http://www.reuters.com/article/us-japan-bitcoin/japans-fsa-gives-official-endorsement-to-11-cryptocurrency-exchanges-idUSKCN1C40T9.

[42] *See, e.g.*, Noelle Acheson, *China's ICO Ban: Understandable, Reasonable and (Probably) Temporary*, COINDESK (Sept. 12, 2017), https://www.coindesk.com/chinas-ico-ban-understandable-reasonable-probably-temporary/; Yuji Nakamura & Sam Kim, *Cryptocurrencies Drop as South Korea Bans ICOs, Margin Trading*, BLOOMBERG (Sept. 29, 2017), https://www.bloomberg.com/news/articles/2017-09-29/cryptocurrencies-drop-as-south-korea-bans-icos-margin-trading.

[43] *See* Sara Hsu, *China's Shutdown of Bitcoin Miners Isn't Just About Electricity*, Forbes (Jan. 15, 2018), https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/#38340cd3369b.

[44] *MAS clarifies regulatory position on the offer of digital tokens in Singapore*, MONETARY AUTHORITY OF SINGAPORE (Aug. 1, 2017), http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx.

[45] Miguel Freitas, *Out in the Open: An NSA-Proof Twitter, Built With Code From Bitcoin And Bittorrent*, WIRED (Jan. 13, 2014), https://www.wired.com/2014/01/twister.

[46] *Id*.

[47] Aaron van Wirdum, *Is Bitcoin Anonymous? A Complete Beginner's Guide*, BITCOIN MAGAZINE (Nov. 18, 2015) https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/.

technology in their business operations should be cognizant of at least the following U.S. federal laws, as they could impact the use of blockchain technology with regard to data privacy.

FEDERAL TRADE COMMISSION ACT ("FTCA")

The FTCA normally deals with prohibiting "unfair or deceptive acts or practice[s]" within the consumer protection sphere.[48] Although the FTCA does not directly mention data privacy, the Federal Trade Commission ("FTC") has applied the FTCA to data privacy violations that are deceptive or unfair.[49] And while the FTC started with a focus on deception, more recent cases have focused on the unfair aspects of data privacy violations.[50] In this regard, FTC guidance on privacy issues specific to Big Data may be of particular interest to blockchain users. Two recent FTC reports, *Data Brokers: A Call for Transparency and Accountability*[51] and *Protecting Consumer Privacy*, [52] each include best practices recommendations for data brokers. Additionally, *Big Data: A Tool for Inclusion or Exclusion*,[53] gives an overview of considerations for Big Data users with regard to using data that has been collected.

ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

The ECPA imposes criminal sanctions for those trying to intercept electronic communication.[54] Title II of the ECPA—the Stored Communications Act ("SCA")—protects communications stored electronically against improper access and wrongful public disclosure,[55] and is aimed in part at protecting individuals' privacy interests in personal and proprietary information.[56]

The SCA applies to an "electronic communication" stored in "electronic storage" facilitated by an "electronic communication service."[57] "Electronic communication" is defined by the Act to include transfer of data.[58] The Act

---

[48] 15 U.S.C. §§ 41-58.

[49] Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 COMPETITION: J. ANTI., UCL & PRIVACY SEC. ST. B. CAL. 89 (2016).

[50] *Id*. The FTC defines an unfair act or practice as one that (1) causes or is likely to cause substantial injury to consumers, (2) is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition. 15 U.S.C. § 45(n).

[51] Fed. Trade Comm'n, *Data Brokers: A Call For Transparency And Accountability* 23-35 (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[52] Fed. Trade Comm'n*, Protecting Consumer Privacy In An Era Of Rapid Change: Recommendations For Businesses And Policymakers A-3* (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[53] Fed. Trade Comm'n*, Big Data: A Tool for Inclusion or Exclusion?* (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[54] 15 U.S.C. §§ 6801-6827.

[55] 18 U.S.C. §§ 2701-2712.

[56] *Kaufman v. Nest Seekers, LLC*, No. 05 CV 6782, 2006 WL 2807177, *4 (S.D.N.Y. Sept.26, 2006) (citing S. Rep. No. 99-541, at 3 (1986)), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3557).

[57] 18 U.S.C. § 2701(a).

defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[59]

GRAMM-LEACH-BLILEY ACT ("GLBA")

The GLBA regulates the use, disclosure, and collection of "nonpublic personal information" that consumers provide to financial institutions.[60] Of particular concern to what may soon be a widely used technology like blockchain is whether a particular person or entity counts as a "financial institution" under the GLBA. Section 6809 of the Act defines "financial institution" as "any institution the business of which is engaging in financial activities as described in section 1843(k) of Title 12."[61] Section 1843(k) of Title 12 defines "financial activities" as "engaging in any activity that the Federal Reserve Board has determined . . . to be so closely related to banking or managing or controlling banks as to be a proper incident thereto." This definition may capture a wide range of entities interested in blockchain technology, such as credit reporting agencies,[62] banks, insurance brokerage firms, and mortgage companies.[63]

THE BANK SECRECY ACT ("BSA")

The BSA mandates that "financial institutions" (a broad category of businesses offering financial services) must collect and maintain information about their customers and share that information with the Financial Crimes Enforcement Network ("FinCEN").[64] In 2013, FinCEN published guidance titled "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," which commented on whether entities that exchange virtual currency for real funds or virtual currency may be subject to the BSA.[65] The FinCEN Guidance creates and defines three categories of persons: "administrators," "exchangers," and "users."[66] Both exchangers, defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency," and administrators, defined as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency" qualify as "money transmitters" and are therefore subject to the BSA's mandates.[67] "Users,"

---

[58] 18 U.S.C. § 2510(12) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce").

[59] 18 U.S.C. § 2510(15).

[60] 15 U.S.C. §§ 6801-6827.

[61] 15 U.S.C. § 6809(3)(A).

[62] *See Trans Union LLC v. F.T.C.,* 295 F.3d 42 (D.C. Cir. 2002).

[63] The FTC provides detailed guidance for complying with the Privacy of Consumer Financial Information Rule of the GLBA on its website. *See* https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.

[64] *See* 31 U.S.C. §§ 5311-5332.

[65] Dept. of the Treasury: Financial Crimes Enforcement Network, FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), *available at* http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [hereinafter "FinCEN Guidance"].

[66] *Id.* at 2.

[67] *Id.* at 2-5.

defined as persons who use virtual currency "to purchase goods or services," are not money transmitters and have no FinCEN compliance obligations, meaning merchants and consumers are likely to be exempted.[68]

Additional federal laws that may be of some interest in connection with data privacy and blockchain technology are the Health Insurance Portability and Accountability Act[69] ("HIPAA," regulating medical information) and the Fair Credit Reporting Act[70] (regulating consumer-reporting information).

GOVERNMENT APPLICATIONS

Although private companies will likely be the first entities to take advantage of blockchain technology, the federal government has also shown an interest in the space, in applications such as the use of blockchains for record keeping. In this manner, the government may opt to use a blockchain with public read access and private write access; or, alternatively, a series of interoperable public and private blockchains to effectuate the same permissions. This type of permissioned setup would help provide security without sacrificing transparency. Governmental use of blockchain technology, however, also implicates any federal statutes that apply to federal governmental action, such as the Freedom of Information Act ("FOIA"), which improves transparency of the federal government by requiring that federal agencies and departments provide public information upon request without any undue delays.[71] That being said, the FOIA may prove obsolete if the U.S. government were to rely on blockchain technology to record public information. Public records would be fully and easily accessible on a blockchain without the need for formal requests, which would allow for faster and more efficient public data retrieval.

Another potential governmental use of blockchain technology is to facilitate electronic voting. In such cases, it may be beneficial to use a blockchain system that has public write access and private read access.[72] Here, a system may be set up so that any user could be given a single private key[73] that allows a single vote, and wherein only the group that set up the blockchain could access the results. Any changes in the ledger would be recorded, and any fraud would be observed and traceable to whomever entered the fraudulent entries.[74] Blockchain use could even prevent ghost voting (voting for deceased or nonexistent individuals) by automatically checking voter registries.[75] Additionally, such a system could enable voting from smartphones, computers, or other devices, thereby increasing voter turnout perhaps dramatically. These advantages could be easily carried over to proxy voting within corporations, making blockchain a valuable technology for business and corporate governance matters as well.

---

[68] *Id.* at 2; *see also* Meghan E. Griffiths, *Virtual Currency Businesses: An Analysis of the Evolving Regulatory Landscape*, 16 TEX. TECH ADMIN. L.J. 303, 311 (2015).
[69] 42 U.S.C. § 1301.
[70] 15 U.S.C. § 1681.
[71] 5 U.S.C. § 552.
[72] Garry Gabison*, Policy Considerations for the Blockchain Technology Public and Private Applications*, 19 SMU Sci. & Tech. L. Rev. 327, 347 (2016).
[73] Generally, blockchains use public key cryptography which, in simplest terms, means a private key is associated with and provides access to a public address on the blockchain.
[74] *See* Gabison, *supra* note 72, at 347.
[75] *Id*. at 348.

Artificial Intelligence

Artificial intelligence, or "AI," is proving to be one of the most dynamic and ubiquitous technologies in use today. From autonomous cars to facial recognition, AI is poised for integration into many aspects of our day-to-day lives. Every year AI becomes smarter, and AI capabilities are increasing at a seemingly exponential rate. As AI approaches human capabilities, it will fall on the legal industry to reconsider current legal frameworks and adjust their applications as needed to the new technology.

INTELLECTUAL PROPERTY AND AI

The major types of intellectual property—patents, trademarks, copyrights, and trade secrets—typically envision an individual (or group of individuals) who creates something useful or valuable. In return, that individual is granted some sort of IP right—a recognition of the individual as the owner of the creation. In the future, sufficiently advanced AI may have the requisite creativity and productivity to conceptualize and produce such creations on its own. The question then is: can AI own intellectual property?

The answer to this question may vary depending on the particular IP regime. For example, the U.S. Copyright Office explicitly states that it "will register an original work of authorship, provided that the work *was created by a human being*."[76] The Copyright Office "will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author."[77] In the AI context, the Copyright Office has not clarified whether works produced jointly by a human and a machine are copyrightable. Arguably, works created by a program without human interaction could be attributed to the human creator of the program, as the work is arguably the ultimate fruit of his or her intellectual labor.[78] Courts have not yet addressed this issue.

Patent law is less explicit when it comes to determining ownership of works created by machines. However, some provisions cast doubt on the ability of machines to independently obtain patent rights. For example, section 101 of The Patent Act provides that "*[w]hoever* invents or discovers any new and useful process, machine, . . . may obtain a patent therefor . . . ."[79] The Supreme Court has interpreted this to mean that "Congress intended

[76] U.S COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 306 (3d ed. 2017), *available at* https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf. See also *Burrow-Giles Lithographic Co.* v. Sarony, 111 U.S. 53, 58 (1884).
[77] U.S COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 313.2 (3d ed. 2017), *available at* https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf.
[78] *See* Andres Guadamuz, *Artificial Intelligence and Copyright*, WIPO Magazine (Oct. 2017), *available at* http://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html.
[79] 35 U.S.C. § 101 (emphasis added).

statutory subject matter to 'include anything under the sun *that is made by man*.'"[80] Additionally, the America Invents Act defines inventor as "the *individual* or, if a joint invention, the *individuals* collectively who invented or discovered the subject matter of the invention."[81] Although these provisions appear to contemplate only humans as inventors, and not machines, no U.S. case or statute has explicitly excluded machines from being patent owners.

Although patent and copyright protection may not apply to works created by machines, trade secret law could provide a vehicle for such protection. Unlike patent and copyright law, trade secret law does not impose requirements based on the nature of the inventor or author. Rather, and as discussed in Chapter 1, a trade secret generally is simply information that is not generally known to the public, holds some economic advantage as a result of being secret, and is the subject of reasonable efforts to maintain secrecy.[82] Valuable information generated by a machine or program could likely be afforded trade secret protection, as long as the information is not disclosed, and meets the other requirements of trade secret status.

LIABILITY FOR AI SYSTEMS

As AI systems advance in capability and become more prevalent, assessing liability for the actions of these systems will present new challenges. For example, in May 2016, Tesla Motors announced the first known death caused by a self-driving car.[83] The car's sensors system failed to detect a large truck ahead, causing the car to collide with the truck at full speed.[84] Possible candidates for liability in this instance could be the designer of the AI, the manufacturer, the programmer, the user, or perhaps even the AI itself. Current legal frameworks, such as product liability, breach of warranty, and negligence could be employed to assess liability, but these doctrines were not created with the specific challenges of autonomous vehicles and AI in mind. Some commenters have advocated that products liability law is best suited to be adapted to the challenges posed by new AI technologies.[85] Others have called national legislation to address the unique challenges AI presents when assessing liability out of concern that uncertainty over the allocation of risk could stunt the development of new AI technologies.[86]

---

[80] *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980) (quoting S.Rep.No.1979, 82d Cong., 2d Sess., 5 (1952); H.R.Rep.No.1923, 82d Cong., 2d Sess., 6 (1952)).

[81] 35 U.S.C. § 100(f) (emphasis added).

[82] *See* Uniform Trade Secrets Act ("UTSA") § 1 (1985).

[83] Danny Yadron & Dan Tynan, *Tesla driver dies in first fatal crash while using autopilot mode*, THEGUARDIAN (June 30, 2016), https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.

[84] *Id*.

[85] John Villasenor, *Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation*, Center for Tech. Innovation at Brookings 15 (April 2014), *available at* https://www.brookings.edu/wp-content/uploads/2016/06/Products_Liability_and_Driverless_Cars.pdf.

[86] Jessica S. Brodsky, Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit The Brakes on Self-Driving Cars, 31 Berkeley Tech. L.J. 851, 877 (2016), *available at* https://scholarship.law.berkeley.edu/btlj/vol31/iss2/19/.

ADMISSIBILITY OF AI IN LEGAL PROCEEDINGS

Liability is not the only aspect of litigation that intelligent machines may transform. It is conceivable that, at some point, AI may act as an "expert witness," testifying and offering opinions in the courtroom. The question then is whether AI judgment will be deemed admissible in court. The use of software at trial may involve issues of hearsay and reliability. But the largest issue with AI judgment in this context is that it may be impossible to explain how the AI arrived at its conclusion. Unlike typical software, which follows a rigid set instructions, AI does not necessarily employ an algorithm that can be used to adequately describe how a deep learning model outputted a certain answer.[87] The algorithm creating the model does not, by itself, explain the state of the machine's training. It may be that the question of AI testimony or evidence in a court proceeding will be addressed under the standard rubric of *Daubert*, which provides a gatekeeping function and threshold for the introduction of human expert testimony in court.[88] The Daubert test includes consideration of issues such as: (1) whether the methods upon which the testimony is based are centered upon a testable hypothesis; (2) the known or potential rate of error associated with the method; (3) whether the method has been subject to peer review; and (4) whether the method is generally accepted in the relevant scientific community.

Courts could potentially approach AI in this same way, and may deem AI opinions reliable and admissible if the underlying model (and perhaps the engineer who created the model) is deemed credible, experienced, testable, reliable, and commonly accepted in the field. Questions could also be raised regarding a party's reliance on opinions offered by an AI engine—for example, an opinion of non-infringement or invalidity of a patent that a defendant may seek to rely on in its defense of a charge of willful infringement in a patent infringement case.

In any event, businesses and lawyers relying on AI opinions should understand and be prepared to explain the underlying model, how the AI was trained, how the AI was successful in the past, and how successful the AI is with new data.

DATA PRIVACY AND AI

Machine learning and automatic planning are two major sectors of AI that require analysis of large datasets. As such, the ability of AI to predict future behavior based on these datasets can raise privacy issues. Already companies are using datasets to predict credit risk, and state prisons use data sets to predict likelihood of recidivism of their prisoners.[89]

---

[87] *See, e.g.*, Will Knight, *The Dark Secret at the Heart of AI*, MIT TECHNOLOGY REVIEW (Apr. 11, 2017), https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/. (One commenter stating "We can build these models . . . but we don't know how they work." Another stating "It might just be part of the nature of intelligence that only part of it is exposed to rational explanation. Some of it is just instinctual, or subconscious, or inscrutable.").

[88] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

[89] Peter Stone, et. al, *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, STANFORD (Sept. 6, 2016), https://ai100.stanford.edu/2016-report/section-iii-prospects-and-recommendations-public-policy/ai-policy-now-and-future/policy.

ETHICAL ISSUES PERTAINING TO AI

Perhaps more than any other emerging technology, intelligent machines will force us to rethink the role of ethics between humanity and our creations. The Legal Affairs Committee of the European Parliament, for example, approved a report calling on the EU Commission for the introduction of ethical guidelines for the use of intelligent robots.[90] The following ethical issues may not be specifically regulated, but they are worth considering and discussing when developing and implementing AI systems.

EMPLOYMENT

As technical advances continue to enable more efficient production of goods and services, governments and companies alike will continue to face difficult decisions surrounding employment. For example, the trucking industry employs millions of people in the U.S. alone,[91] and as autonomous vehicles become commercially viable, some have begun to question the impact the technology will have on employment.[92] While the ultimate impact of technology on the labor force is debated by economists, companies should be mindful of the publicity and political risks associated with AI projects that have the potential to displace large swaths of the human workforce.

UNINTENDED CONSEQUENCES

In some situations, machines may carry out commands in a manner not initially conceived of by its programmers.[93] For example, should an autonomous vehicle designed to protect human life be able to decide who lives and dies in a car accident?[94] In this regard, businesses must be aware of the unpredictability of AI and avoid open-ended instructions that may be misconstrued.

BIAS AND DISPARATE IMPACT

Other concerns can arise from the use of AI systems, including with respect to unintended bias and disparate impacts on certain classes. For example, companies deploying AI systems will want to ensure that issues related to protected classes like race and gender do not ultimately drive AI-generated decisions.

As one simple example of the risks that can be presented by AI bias, in March 2016, a machine called "Beauty.AI" was created to purportedly judge photographs of people based on facial beauty. Nearly all the winners were

---

[90] 22 No. 3 Cyberspace Lawyer NL 1.

[91] Julia Bossmann, *Top 9 ethical issues in artificial intelligence*, WORLD ECONOMIC FORUM (Oct. 21, 2016), https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/.

[92] *See* Anita Balakrishnan, *Self-driving cars could cost America's professional drivers up to 25,000 jobs a month, Goldman Sachs says*, CNBC (May 22, 2017), https://www.cnbc.com/2017/05/22/goldman-sachs-analysis-of-autonomous-vehicle-job-loss.html.

[93] Bossmann, *supra* note 91.

[94] Keith Naughton, *Should a Driverless Car Decide Who Lives or Dies?*, BLOOMBERG BUS. (June 25, 2015), http://www.bloomberg.com/news/articles/2015-06-25/should-a-driverless-car-decide-who-lives-or-dies-in-an-accident.

white, despite the far more diverse and international pool of candidates, because the training dataset contained many more images of white people.[95] Whether liability should be imposed for biased AI is an ongoing question.

The FTC has expressed some concern about the potential for disparate impact of AI systems, for example, in its 2016 report "Big Data: A Tool for Inclusion or Exclusion?"[96] Surely these concerns will remain at the fore for the FTC and others.

UNMANNED/AUTONOMOUS VEHICLES

Unmanned or autonomous vehicles are a particular implementation of AI technology that is projected for massive growth in the coming years, and which has the potential for dramatic impacts on society. Autonomous automotive technology has experienced rampant development in recent years, with one notable advocate, Elon Musk, predicted that Tesla cars will be able to drive, autonomously, from one U.S. coast to the other by 2018.[97] Although autonomous vehicles raise many of the same concerns as do other AI applications, there are a number of additional considerations specific autonomous vehicles. Accordingly, it is likely that regulatory frameworks will explicitly address the autonomous vehicle industry. The following frameworks and guidance have already been provided to date.

U.S. DEPARTMENT OF TRANSPORTATION ("USDOT")

In September 2016, the USDOT released a policy report that provides guidelines for a regulatory framework for autonomous cars.[98] Signaling that the federal government will embrace autonomous vehicle technology, the report outlines safety expectations and encourages the creation of uniform, national rules. The report provides guidance across four areas: vehicle performance standards, state and federal policy, use of current regulatory

---

[95] Ben Plomion, *Does Artificial Intelligence Discriminate?*, FORBES (May 6, 2017), https://www.forbes.com/sites/forbescommunicationscouncil/2017/05/02/does-artificial-intelligence-discriminate/#30ae2a7730bc.

[96] Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion?* (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[97] Marla Aufmuth, *Elon Musk: Tesla's Autonomous Car Will Drive Coast-To-Coast by 2018*, FUTURISM (May 22, 2017), https://futurism.com/elon-musk-teslas-autonomous-car-will-drive-coast-to-coast-by-2018/. Tesla also recently reiterated its goal to reach this milestone in the near future. Ryan Felton, *Tesla Thinks It Can Do A Coast-To-Coast Autonomous Drive Within The Next 3-To-6 Months (UPDATED)*, JALOPNIK (Feb. 7, 2018) https://jalopnik.com/tesla-still-wants-to-do-a-coast-to-coast-autonomous-dri-1822815014.

[98] National Highway Traffic Safety Admin., *Federal Automated Vehicles Policy* (Sept. 2016), *available at*https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf; *see also* Hope Reese, *US DOT unveils 'world's first autonomous vehicle policy,' ushering in age of driverless cars*, TECHREPUBLIC (Sept. 20, 2016), http://www.techrepublic.com/article/us-dot-unveils-worlds-first-autonomous-vehicle-policy-ushering-in-age-of-driverless-cars/.

tools, and suggestions for new regulatory tools.[99] The report places particular emphasis on safety and sustainability.[100]

STATE LAWS REGARDING AUTONOMOUS CARS

Currently, twenty-one (21) states have passed legislation related to autonomous vehicles, with Nevada being the first in 2011. As an example, Nevada's legislation explicitly allows operation of fully autonomous vehicles, conditioned on certain requirements.[101] The legal framework in the U.S., however, still remains a rough patchwork at this point, with little in the form of uniform standards.

FAA MODERNIZATION AND REFORM ACT ("FMRA")

In 2012, Congress enacted the FMRA, which gave the Federal Aviation Administration ("FAA") control over regulation of unmanned aerial vehicles ("UAVs").[102] Under the act, the FAA can take action against those who conduct unauthorized UAV operation. For example, in 2016, the FAA released regulations on commercial drones "designed to minimize risks to other aircraft and people and property on the ground."[103] The regulations cover piloted drones as well as unmanned drones weighing less than 55 pounds used for routine non-hobbyist use.[104]

---

[99] Cecelia Kang, *Self-Driving Cars Gain Powerful Ally: The Government*, THE NEW YORK TIMES (Sep. 19, 2016), https://www.nytimes.com/2016/09/20/technology/self-driving-cars-guidelines.html?mtrref=en.wikipedia.org&mtrref=undefined&gwh=86074D952DB2F14FDB427B34E1B695D6&gwt=pay.

[100] *Id*.

[101] *Autonomous Vehicles*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Sept. 21, 2017), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.

[102] Pub. L. No. 112–95, 126 Stat. 11 (codified at 49 U.S.C. § 40101 note).

[103] *See New FAA Rules for Small Unmanned Aircraft Systems Go Into Effect*, FED. AVIATION ADMIN. (Aug. 29, 2016), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20734; *see also* James Vincent, *FAA regulations for commercial drones are now in effect*, THE VERGE (Aug. 30, 2016), https://www.theverge.com/2016/8/30/12707502/drone-regulations-legality-us-faa.

[104] *Id*.

Biometric Data

The commercial use of biometric data—data regarding people's physical being—has increased at a rapid rate in recent years. Fingerprints are a well-known example of biometric data that is commonly recorded and used. Other uses involve facial recognition, retinal scans, voiceprint reading, and keystroke analysis. Although the field of biometrics is limited today by our current methods of collection, the list of mechanisms for collecting and using biometric data continues to quickly expand.

PRIVACY IMPLICATIONS FOR BIOMETRIC DATA

Any discussion on the collection and use of biometric data necessarily implicates privacy concerns. The point is summarized well by a dissenting opinion of a decision in a biometric data criminal case upholding a life sentence based on swiped DNA: "[t]he Majority's approval of such police procedure means, in essence, that a person desiring to keep her DNA profile private, must conduct her public affairs in a hermetically sealed hazmat suit."[105]

Currently, various laws in the U.S. touch directly on biometric data, or may be otherwise relevant as broad privacy laws. The most stringent of these is an Illinois state law known as the Biometric Information Privacy Act ("BIPA").[106] Generally, the BIPA: (1) requires informed consent prior to collection; (2) prohibits profiting from biometric data; (3) permits only a limited right to disclose; (4) mandates protection obligations and retention guidelines; and (5) creates a private right of action for individuals harmed by violators of the BIPA.[107] The BIPA gives any harmed individual a private right of action, and entitles a prevailing party to statutory damages for each violation equal to: the greater of $1,000 or actual damages for negligent violation of the BIPA; or, the greater of $5,000 or actual damages for intentional or reckless violation of the BIPA.[108]

The BIPA has spawned a rash of class action lawsuits against employers in a number of different industries, some of which allege that employers use time clocks to collect and use biometric information—including fingerprints and hand scans—in a manner that violates the statute's consent and notice requirements. Similar suits have been filed against social networking and photo sharing websites that provide, e.g., facial recognition functionality for identifying the subjects in photographs uploaded to the services, given that facial recognition is specifically recited (as "face geometry") as one of the biometric identifiers within the BIPA's scope.[109] Statutes like the BIPA could

[105] *Raynor v. State*, 440 Md. 71, 108, 99 A.3d 753, 775 (2014).

[106] Amy Korte, *Airlines Hit with Class-Action Lawsuits Under Biometric Privacy Law*, ILLINOIS POLICY (Nov. 20, 2016), https://www.illinoispolicy.org/united-airlines-hit-with-class-action-lawsuit-under-biometric-privacy-law/.

[107] Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, AMERICAN BAR ASSOCIATION (May 2016), https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

[108] *Id*.

[109] Korte, *supra* note 106.

have a significant impact on facial recognition in video as that technology is deployed on a broader scale across Big Data and AI systems.

As of 2017, only two other states, Washington and Texas, have enacted laws governing biometrics that are as encompassing as the BIPA. Both states have largely emulated the BIPA; however, unlike the BIPA, their respective versions do not provide a private right of action—only the attorney general can enforce these biometrics laws.[110] A number of other states, including Alaska, Connecticut, Montana, and New Hampshire, have considered similar legislation,[111] and given the proliferation of biometric data collection and use, it is only a matter of time before more states adopt similar laws. Currently, there is no comprehensive federal statute governing the collection, protection, use, or disposal of biometric data.

California law prohibits operators of websites geared towards K-12 school purposes from selling students' biometric data and restricts use of that data.[112] Illinois law prohibits school districts from collecting biometric information from students without parental consent, mandates that its districts stop using such information when a student graduates, leaves the school district, or when a written request is received from the student, and requires that all biometric information be destroyed within 30 days of discontinued use. Further, districts may only use biometric information for student identification or fraud prevention, and may not sell or disclose to third parties without parental consent or pursuant to a court order.[113] At least Wisconsin, Louisiana, Arizona, and Kansas have similar laws.

The FTC provided a useful guide for practices in connection with facial recognition technology in its report *Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies*.[114] The report focuses on privacy concerns, and generally suggests that companies should collect only the personal data they need, should remove that data as soon as they no longer need it, should securely store it and limit third-party access to it, and should inform users when their data is linked to or shared with third parties.[115] Notably, the report outlines two scenarios in which companies should seek consumers' affirmative consent before using facial recognition data: first, before using facial recognition data in a different way than what was initially represented; and, second, before using facial recognition data to determine the identity of a person, in an otherwise anonymous image, for an entity that could not otherwise identify the person on its own.[116] Companies should take note of the FTC's suggestions, as the FTC

---

[110] Hanley Chew & Jonathan S. Millard, *Washington Joins Illinois and Texas In Enacting Biometric Data Law*, MONDAQ (July 3, 2017), http://www.mondaq.com/unitedstates/x/607328/Data+Protection+Privacy/Washington+Joins+Illinois+And+Texas+In+Enacting+Biometric+Data+Law.

[111] *Id*.

[112] *Id*.

[113] *Id*.

[114] Fed. Trade Comm'n, *Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies* (Oct. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[115] *Id*.

[116] *Id*.

hints that a company's failure to follow proper business practices with regards to facial recognition could subject it to FTC sanctions.[117]

[117] Claypoole & Stoll, *supra* note 107.