Issue 03 February 2021

BakerHostetler

Pivot. Accelerate. Transform.

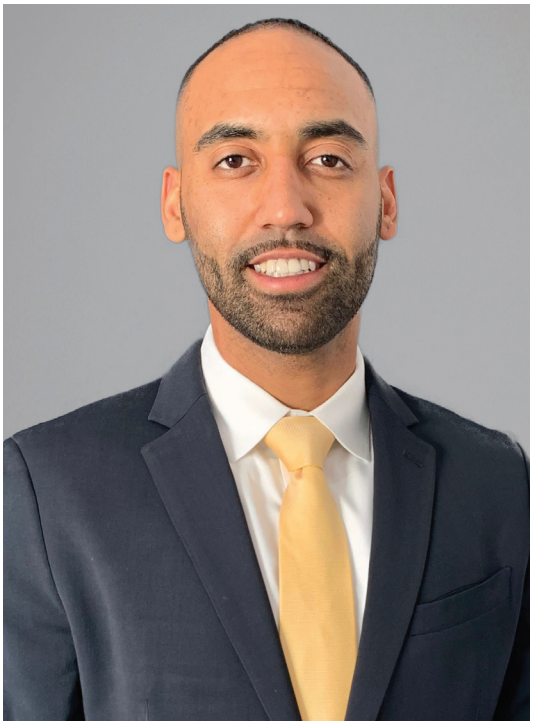
Welcome

Across the economy, businesses are using digital technology to pivot into innovative service lines, accelerate growth and transform. A business's digital strategies and data assets play an important role in its success.

Digital transformation means, among other things, deploying the latest technologies – including artificial intelligence (AI) and automated decision-making. However, advances in AI raise fundamental legal and ethical questions. Not surprisingly, there is much debate on how and when to regulate the use of AI. While there is no comprehensive "AI law" in the U.S., there are many current and proposed laws related to the use of AI. It is important for businesses to understand this evolving landscape so they can identify risks during digital transformation – particularly in the areas of notice, transparency and data privacy.

In this issue, we are highlighting Stanton Burke and how his practice advises clients on the legal requirements and ethical considerations when using these technologies.

Spotlight



Stanton Burke addresses legal and ethical considerations when deploying AI.

In the U.S., we have a fragmented and complex set of federal and state legal and regulatory requirements that businesses need to be aware of when developing digital transformation strategies or deploying new technologies, like AI. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices. This essentially requires a business to provide consumers with notice and transparency about data handling practices, including disclosures around the use of personal information (PI). For example, if a business makes a material misrepresentation or omission about its business practices (such as how it processes personal data or uses AI), the FTC has broad authority to bring an enforcement action against it for failing to adhere to its own stated assurances and privacy policies, particularly if it causes consumer harm. As such, businesses should ensure that the use of personal data, including in AI models, is consistent with its assurances and aligns with consumers' reasonable expectations.

The California Consumer Privacy Act has extensive notice requirements, including pre-collection notice and detailed privacy policy requirements. For example, a business's processing of inferential data, which is common in AI models, would require disclosure in the privacy policy, including how this category is used and whether it is shared or sold. Under the forthcoming California Privacy Rights Act (CPRA), consumers have the ability to opt out of the sharing of their PI, opt out of automated decision-making

Spotlight (cont'd.)

and profiling, correct their PI, and limit the use of their sensitive PI. Under the CPRA, additional regulations will be issued governing access and opt-out rights with respect to the business's use of automated decisions – including requiring disclosure of meaningful information about the logic involved in the decisions and the likely outcome of the process.

In Europe, under the General Data Protection Regulation (GDPR), to meet the explainability principle, companies should be able to adequately explain the decisions made using personal data. Also, under Article 22 of the GDPR, businesses must provide the ability for consumers to opt out of decisions made solely based on AI that result in "legal effects or similarly significant effects." This essentially requires a three-step process: (1) assessing whether the deployment of AI is "solely automated," (2) assessing whether the decision-making use case constitutes a "legal or similarly significant effect" and (3) if so, and if no exceptions apply, enabling the data subject to opt out and not be subject to the decision.

As a practical matter, notice and transparency requirements should be broad enough to cover foreseeable uses of AI to avoid having to provide additional notices or seek new consent as a result of an omission. Also, it is important to assess the extent to which these regulations apply, given that there are several exceptions. There are many other regulations that implicate AI that this issue will not cover in detail, including Title VII, Copyright Laws, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and various biometric laws and additional global privacy regimes. For example, under Title VII, businesses that use AI for hiring can be held liable for discriminatory results, which requires careful consideration when using AI to evaluate applicants. Regarding copyright protection, although raw data is not subject to protection in the U.S., the original selection and arrangement of the facts (i.e., databases) can be protected. Therefore, if a business were to develop proprietary AI software, it should format and protect the applicable IP aspects to the extent possible.

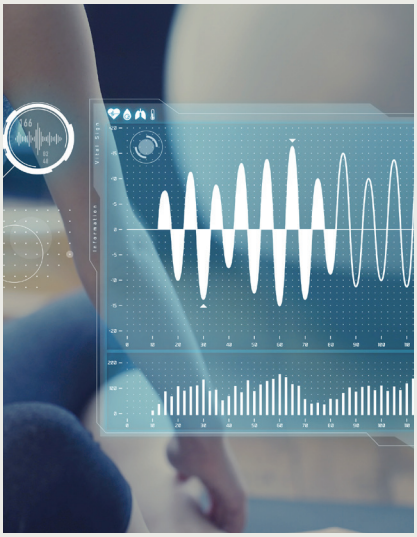
My goal when counseling on the deployment of transformative technologies is to advise not only on the legal requirements but also on the ethical considerations. We often get asked by clients what they "should" do as it pertains to the use of AI, given the lack of clarity in the legal landscape. While these are ultimately business decisions, it is the lawyers who are increasingly tapped for their judgment on these issues. For example, ethical questions often arise as to how a business might use AI for commercial purposes, whether to use open source or proprietary data sets for AI models, what contractual measures to put in place when engaging with vendors of AI tools, whether the business's current notices adequately capture a transformative use case, or how to evaluate the risk of an algorithm resulting in unfair bias. As businesses build return-to-work strategies, additional questions arise, such as how to leverage tools on company systems for employee monitoring to assess work-from-home productivity, how to deploy AI-powered facial recognition for contact tracing, and the extent to which notice and consent is required for it. The DTDE team is well positioned to address the legal components for all of these questions as well as ethical factors such as fairness, integrity, and alignment with core values and brand reputation.

I recommend that legal and technical teams partner with outside counsel to create an AI framework that outlines the company's ethical posture and offers guidelines that balance innovation and responsibility. It should cross-reference and align with other applicable company policies and procedures, including privacy policies, privacy and vendor risk assessments, data retention policies, and information security programs. It should include the rules of the road when leveraging AI. For example, avoid using data sets without the proper IP rights, avoid deploying AI in ways that conflict with privacy notices or cause consumer harm, routinely audit databases and models for unfair bias, and consider the nature and sensitivity of the data sets. In summary, the creation of an AI framework is an excellent opportunity to align legal and technical teams, operationalize technology principles, and analyze the legal and ethical implications of digital transformation.

OF RECENT NOTE

Client Alerts

ONC's New Guidance Helps Further Clarify Application of the Information Blocking Rules



Blog Posts

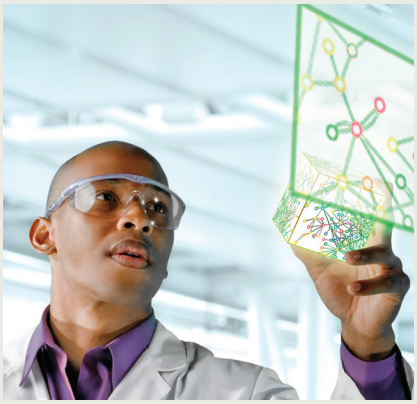
Court Finds HHS Had No Lawful Basis Under HIPAA for a $4.3 Million Civil Money Penalty: What Does This Mean for Future HHS Enforcement Actions?

Happy First Birthday to the NIST Privacy Framework!

Compliance and Cybersecurity Best Practices Rewarded with HIPAA Safe Harbor

Podcasts

The Digital Health Ecosystem



Emerging Issues

Is ethical risk getting the better of artificial intelligence?, Tech HQ, Feb. 2, 2021

There are too many cases of discrimination in AI and, in some cases, organizations are even shelving plans to adopt it altogether.

AI Ethics Really Come Down to Security, *Forbes,* Jan. 27, 2021

It's expected that there will be 75 billion smart connected devices in our homes and offices by 2025, and many of them will have added capacity to sense, process and make decisions without first checking with the cloud — or with us. If we're going to rely on them to take more active and responsible roles in our lives, we must be able to trust that they're not only ethical but that the AI and the machine learning that underpins them operate safely and securely.

6 developments that will define AI governance in 2021, *Brookings,* Jan. 21, 2021

This year is poised to be a highly impactful period for the governance of AI. The Trump administration successfully pushed for hundreds of millions of dollars in AI research funding, while also encouraging the formalization of federal AI practices. President Joe Biden will start his new administration with federal agencies already working to comply with executive guidance on how to use and regulate AI.

Beyond passing the AI spending increases, Congress also tasked the White House with creating a new National AI Initiative Office to orchestrate these developments. All this comes as the European Commission (EC) has put forth the Digital Services Act, which will create oversight for how internet platforms use AI. The EC is also poised to propose a comprehensive approach to AI safeguards in the spring. Taking all this into account, 2021 promises to be an important inflection point for AI policy.

The AI Incident Database wants to improve the safety of machine learning, *TechTalks*, Jan. 14, 2021

The AI Incident Database aims to make it easier to see past failures and avoid repeating them.

The AIID is sponsored by the Partnership on AI (PAI), an organization that seeks to develop best practices on AI, improve public understanding of the technology, and reduce potential harm AI systems might cause. PAI was founded in 2016 by AI researchers at Apple, Amazon, Google, Facebook, IBM, and Microsoft, but has since expanded to include more than 50 member organizations, many of which are nonprofit.

FDA action plan puts focus on AI-enabled software as medical device, *Healthcare IT News*, Jan. 14, 2021

The agency plans to take a "multi-pronged approach" to advancing oversight of machine learning-enabled devices – with an eye toward ensuring patient safety, algorithm transparency and real-world results.

National AI Initiative Office launched by White House, *Fed Scoop*, Jan. 12, 2021

The White House on Tuesday fulfilled its requirement to establish an office responsible for coordinating artificial intelligence research and policymaking across government, industry and academia.

Dubbed the National AI Initiative Office, it will implement a national AI strategy under the leadership of Founding Director Lynne Parker, who also serves as U.S. deputy chief technology officer.

How the Pentagon's AI Center Aims to Advance 'Responsible AI Literacy' in 2021, *Nextgov,* Jan. 12, 2021

In 2021, the Pentagon's Joint Artificial Intelligence Center intends to further push forward foundational guidance and projects promoting responsible AI use and strengthened awareness across the entire Defense enterprise—and the National Defense Authorization Act contained a few mandates that could support those fresh efforts.

Unstructured Privacy Data Risks: AI Can Help, *CPO Magazine,* Jan. 8, 2021

As per Gartner, 65% of world population's data will be impacted due to privacy regulations by 2023. It might happen sooner as most countries wish to provide economic nationalism by restricting cross country data transfers and data rationing by global technology businesses.

Another Independent trend coupled with the rise of tighter privacy regulations is the volume of unstructured data being collected. it is estimated that about 60-80% of the overall data stored today is unstructured. Combined, both structured & unstructured data are projected to grow at the rate of 7-12% on an annual basis.

Prestigious AI meeting takes steps to improve ethics of research, *Nature,* Dec. 23, 2020

After a year of heavy scrutiny and seemingly endless controversy around AI technologies, the field's most prestigious conference has tried to set a good example. For the first time, the Neural Information Processing Systems (NeurIPS) meeting, which took place completely online this month, required presenters to submit a statement on the broader impact their research could have on society, including any possible negative effects.

Data Skills Catalog and Data Ethics Framework Now Available, GSA Technology Transformation Services, Dec. 1, 2020

The mission of the Federal Data Strategy (FDS) is to fully leverage the value of federal data for mission, service, and the public good. As part of the FDS 2020 Action Plan, the General Services Administration (GSA) committed to complete Action 13: Develop a Curated Data Skills Catalog (Catalog) and Action 14: Develop a Data Ethics Framework (Framework).

Who is an AI Ethicist and What Does He / She Do, *Digit,* Jul. 13, 2020

As artificial intelligence and machine learning solutions take over every facet of our lives, it is being observed that users' trust in them has been plummeting at a slow but steady rate. According to Gartner, multiple incidents of astounding privacy breaches and data misuse have led to the growing dissonance between AI solutions and their consumers.

Regulatory scrutiny for AI is rising across the world, in order to combat such breaches. Despite these efforts, Gartner predicts that 75 per cent of large organizations dabbling in AI will hire "AI behavior forensic, privacy and customer trusterest", in simple words - an AI ethicist, by 2023 to diminish brand and reputation risk.

Decision Points in AI Governance, *Center for Long-Term Cybersecurity: UC Berkley,* May 5, 2020

This report issued by The Center for Long-Term Cybersecurity (CLTC) takes an in-depth look at recent efforts to translate AI principles into practice. The report, Decision Points in AI Governance, authored by CLTC Research Fellow and AI Security Initiative (AISI) Program Lead Jessica Cussins Newman, provides an overview of 35 efforts already under way to implement AI principles, ranging from tools and frameworks to standards and initiatives that can be applied at different stages of the AI development pipeline.

Using Artificial Intelligence and Algorithms, *ftc.gov,* Apr. 8, 2020

Headlines tout rapid improvements in artificial intelligence technology. The use of AI technology – machines and algorithms – to make predictions, recommendations, or decisions has enormous potential to improve welfare and productivity. But it also presents risks, such as the potential for unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities.

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, *European Commission,* Aug. 8, 2018

The GDPR introduces new provisions to address the risks arising from profiling and automated decision-making, notably, but not limited to, privacy. The purpose of these guidelines is to clarify those provisions.