SHARE:

Join Our Email List

View as Webpage

July 20, 2022

Welcome

Welcome to the 14th issue of *Decoded* for the year.

In addition to the several topics we cover in this edition, we drilled down and took a deep dive regarding the American Data Privacy and Protection Act. What is it? Where does it stand? What impacts will it have on various industries? Alex Turner and Kelsie Wiltsie take us behind the curtain and provide their insights on how this piece of legislation could be a game changer.

We hope you enjoy this issue and, as always, thank you for reading.

Nicholas P. Mooney II, Co-Editor of *Decoded,* Chair of Spilman's Technology Practice Group, and Co-Chair of the Cybersecurity & Data Protection Practice Group

and

Alexander L. Turner, Co-Editor of *Decoded* and Co-Chair of the Cybersecurity & Data Protection Practice Group

---

Is the U.S. Finally Getting a Comprehensive Cybersecurity and Data Protection Law? What You Need to Know About the Proposed American Data Privacy and Protection Act

By Alexander L. Turner and Kelsie A. Wiltsie

In the beginning of the 2000s, as a result of the advance in technology, the Federal Trade Commission looked to Congress to pass legislation that would ensure protection of citizens' privacy rights. However, Congress thus far has been unable to pass comprehensive privacy protection legislation, leaving it instead to the states to pass their own such legislation in a piecemeal fashion. On the other hand, in 2018, the European Union passed the General Data Protection Regulation ("GDPR"), which is

comprehensive throughout the EU and takes a firm stance on data privacy and security, imposing obligations on businesses and organizations that collect consumer data, and levying large fines for violations of the regulation.

In June 2022, Representatives Frank Pallone (D-NJ), Cathy McMorris Rodgers (R-WA), and Senator Roger Wicker (R-MS) introduced the American Data Privacy and Protection Act ("ADPPA"). The ADPPA will be the nation's first comprehensive consumer data privacy and security framework, if passed. This bill is largely modeled after the GDPR, with a few key differences, and incorporates provisions from previously failed privacy legislation. The ADPPA covers a broad range of substantive areas, including child privacy, data breach/security, health care, and internet/mobile app privacy.

Click **here** to read the entire article.

New Virginia Law Lets Local, Campus Police Use Facial Recognition Technology. How Can They Use It?

"There are 14 circumstances in which state, local and campus police will be allowed to use the technology."

Why this is important: In Virginia, campuses now have access to a new tool to assist them in conducting investigations. On July 1, 2022, amendments to two Virginia statutes took effect that now permit local and campus police to use facial recognition technology without the need for a warrant. This tool was previously only available to the Virginia State Police. Pursuant to the new statute, campus police may use facial recognition technology to:

- Help identify an individual where there is a reasonable suspicion the individual has committed a crime;
- Help identify a crime victim, including a victim of online sexual abuse material;
- Help identify a person who may be a missing person or witness to criminal activity;
- Help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife;
- Help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking;
- Help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood;
- Help identify a deceased person;
- Help identify a person who is incapacitated or otherwise unable to identify himself;
- Help identify a person who is reasonably believed to be a danger to himself or others;
- Help identify an individual lawfully detained;
- Help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism;
- Ensure officer safety as part of the vetting of undercover law enforcement;
- Determine whether an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other official forms of identification using information that is fictitious or associated with a victim of identity theft; and
- Help identify a person who an officer reasonably believes is concealing his true identity and about whom the officer has a reasonable suspicion has committed a crime other than concealing his identity.

While the technology can be used as a "lead generator," it cannot be used in order to establish probable cause as a basis for a search warrant. The statute also contains escalating criminal penalties for misuse of this technology.

Despite these safeguards, privacy concerns remain. One of those concerns is misidentification. While the statute requires that the technology used be 98 percent accurate as determined by the National Institute of Standards and Technology, the technology is not infallible. The accuracy of the facial recognition technology is usually tested in a controlled environment and not in the real world. Privacy advocates are concerned that use of this technology in the real world where variables are not controlled will disproportionally impact individuals with darker skin. The use of this technology by local and campus police will have to be studied to determine its overall effectiveness. Critics are also concerned that the use of this technology without a warrant would constitute a violation of an individual's Fourth Amendment rights insofar as individuals did not concede to have their image used by this technology just because they posted a picture to social media or walked past a CCTV camera. Only time and anticipated

court challenges will determine if access to this new investigatory tool will continue to be permitted. --- Alexander L. Turner

---

CureVac NV Sues BioNTech for IP Infringement

"CureVac filed a lawsuit in the German Regional Court in Düsseldorf against BioNTech SE and two of its subsidiaries, seeking compensation for infringement of CureVac's patents that cover mRNA modification and expression levels as well as mRNA vaccine formulations specific to SARS CoV-2 vaccines."

Why this is important: This is a lawsuit to watch. We do not have "the facts," except what the complaint alleges. CureVac NV, a Dutch/German developer of an ineffective COVID-19 vaccine, is suing the developer and manufacturer of Pfizer's effective vaccine for patent infringement. BioNTech was developing RNA drugs when it was acquired by Pfizer to develop the COVID-19 vaccine. Moderna was making similar strides here. CureVac alleges that some of the technology used by BioNTech actually belonged to CureVac. Sour grapes or stolen grapes? We may not know for some time. FYI, our understanding of the Moderna patent is that it uses a similar, but technologically distinct process. It is not overlapping with the BioNTech patent, to my knowledge. We do not know if it could be impacted by the CureVac NV patent claim. --- Hugh B. Wellons

---

3D 'Bioprinting' Could Help with Child Heart Defects and More

"Most tissues created through bioprinting to date are quite small – and nearly all are still in different phases of testing."

Why this is important: For a child with a heart defect (impacting approximately one percent of children born in the United States), every second counts. Medical interventions for these conditions have existed for many years. Longitudinal data have shown that a major setback to full recovery is that repeated intervention is needed as children quickly outgrow their mechanical devices and implants. Bioprinting offers a promising solution as bioengineers work to develop the ability to print heart tissue that can grow with the patient. Time has been a large hurdle. There are hundreds of millions of cells in a single millimeter of human heart tissue. Bioprinters struggle to keep up with research demand as historically it can take weeks to produce a very small amount of usable tissue. A team of researchers in Stanford University's bioengineering labs, led by Mark Skylar-Scott, Ph.D., have developed a method of working with clusters of stem cells called "organoids" which act like building blocks to combine with other organoids as a quicker means of manufacturing organ tissue. By working with clusters of cells, rather than individual cells, the goal is to have tissue structures that dynamically interact with the patient's existing structures, and effectively "grow" with the patient. While still in very early stages, researchers continue to look for ways to scale up productions to the amount needed for developing workable tissue structures. These developments present very interesting legal issues and opportunities in protecting intellectual property in the lab-grown tissue technology markets. While patent applications with claims related to organoids have been around since the early 2000s, the development market saw its largest growth starting around 2014. This is an important opportunity zone for developing unique processes, devices, testing methods, culture vessels and media, screening compounds and end-use applications for organoid technologies. --- Brian H. Richardson

---

The Great Cybersecurity Resignation

"This is a problem that all organisations now face, but in the Cybersecurity sector this is becoming an increasingly worrying issue that Boards now need to face up to."

Why this is important: This article discusses how The Great Resignation affects chief information security officers and others in the cybersecurity sector. Readers of *Decoded* will remember that we recently reported on the tug-of-war among cybersecurity personnel being required to do more with less, the increased frequency and sophistication of cyberattacks, and the often old and unsecure networks systems used by employees working from remote locations. This article reports that CISOs and cybersecurity employees are leaving in droves, and one of the primary reasons for this is the search for better work-life balance. Also, remote work now makes it possible for employees to work for the competition not only in the same locale, but across the country. The result in the workplace is a shift of

power from employer to employee, and the same is true for cybersecurity employees. --- Nicholas P. Mooney II

Cryptocurrency Increasingly Used in Drug, Human Trafficking

"Criminals can now use a kiosk — a machine similar to an ATM — to transfer large sums of money with ease and anonymity."

Why this is important: As law enforcement agencies seek to combat drug trafficking and online sex trafficking, they must also have an understanding of how the money is flowing. Sophisticated illegal operations are using cryptocurrencies to facilitate their operations. According to the Homeland Security and Justice Team in the Government Accountability Office, such currencies are being used as a mode of payment in drug trafficking because of the perceived anonymity and the ease of the movement across international borders. The traffickers no longer need to drop off large cash bags to complete their transactions as they can now use a kiosk to complete money transfers. Law enforcement will need to ensure that they have an understanding of cryptocurrency as well as the patterns and practices of these illegal operations. --- Annmarie Kaiser Robey

---

Rising Application of CRISPR Genome in Different Fields of Biotechnology is Driving Genome Editing Market Revenue Growth and 'Softer' Form of CRISPR May Edit Genes More Accurately and A Potential Danger of CRISPR Gene Editing—and Why Base Editing May be Safer

"Rapid advancements in gene-editing technologies, increasing investment by governments and private entities in biotechnology and biomedical research, and increasing application of gene-editing technology in fields such as gene therapy, therapeutics, mutations, agricultural biotechnology, and others are some other key factors expected to continue to drive revenue growth."

"Gene editing with CRISPR can cause off-target mutations, but this seems to happen less often with an enzyme that cuts one of the strands of DNA instead of both."

"A report from Boston Children's Hospital warns of a potential, previously undiscovered danger of CRISPR editing."

Why this is important: I apologize for harping consistently on CRISPR, but it will change our world as we know it. New developments in this technology will accelerate that change. We already see in the einnews.com article an "industry" that seems somewhat independent of the market, due to its promise. The biotech market, in general, is a bit down. Gene editing support seems to be up! The second article, from newscientist.com, talks about one of the new improvements to CRISPR that make it less of a blunt tool. The third article describes a danger of CRISPR. CRISPR, especially combined with more traditional gene therapy, eventually will reduce inherited diseases and conditions, extend lives, etc. Although not entirely "ready for Prime Time," it is a technology largely for good. My concern is that we are not spending enough time and thought on the current accuracy of the technique and the negative effects, especially how to minimize those. --- Hugh B. Wellons

---

Diabetes Patients Flood FDA with Comments on Cybersecurity for Medical Devices

"The FDA is under pressure from Congress to improve the cybersecurity of medical devices through its pre-market approval process."

Why this is important: July 7, 2022 marked the closing of the open period for comments on the updated FDA guidance for "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions." This draft guidance is an update to the previous 2018 version, and implements certain additions and revisions consistent with the PATCH Act to address total life cycle

cybersecurity concerns in medical devices. More than 1,000 comments were received from diabetes patients and caregivers. The Centers for Disease Control and Prevention estimates that approximately 10 percent of the United States population has diabetes. The comments received are representative of an important population in the health care and medical device market. A trend in the comments received reveal that diabetes patients and medical device users are very concerned that the updated regulations and cybersecurity measures could impact the individual patient's access to control their devices. Comments are specifically asking that the FDA include clarification that states a patient user's access to and control or use of their own medical device should be considered "authorized' access, and not be deemed a cybersecurity threat. Their concerns are similar to other industries where consumers are advocating for a "right to repair" such as with document printers that lock out printing unless a proprietary ink cartridge is used. These concerns are well founded, and patients are certainly correct to be concerned that their access to full control of their own lifesaving devices would be curtailed in any way. However, we have frequently seen, and cybersecurity professionals agree, that end user human error is still the leading cause of a cybersecurity breach. Any guidance language that would grant fully "authorized" device access to an device user should be accompanied by adequate training, boundaries, and protections to limit the high risk of adverse effects caused by inadvertent human error. --- Brian H. Richardson

---

Cyber Incident Reporting Law Takes Effect in Virginia

"The law adds Virginia to a growing list of states to impose reporting requirements on agencies and local governments."

Why this is important: A few weeks ago, Virginia joined Indiana, New Hampshire, and West Virginia in requiring the Commonwealth's agencies and local governments to report cybersecurity incidents. Senate Bill 764, which took effect at the end of June, requires every public entity in Virginia to report all data breaches, compromises of data security, exposures of protected information, or disruptions of IT systems to the Virginia Fusion Intelligence Center, who is then to report the incident to the Virginia's Chief Information Officer ("CIO"). The CIO is also required to convene a work group to review current cybersecurity reporting and information sharing practices and report any legislative recommendations to the Governor and the Chairmen of the Senate Committee on General Laws and Technology and the House Committee on Communications, Technology and Innovation. The new law also prohibits any government entity from using any hardware, software, or services that have been prohibited by the U.S. Department of Homeland Security for use on federal computer systems. --- Alexander L. Turner

---

Sci-Fi No More: Synchron Implants Mind-Reading Device in First US Patient in Paralysis Trial

"The first U.S. clinical trial of a brain implant that returns the power of communication to severely paralyzed people has begun."

Why this is important: Synchon developed and put into clinical trials an implant that is relatively noninvasive in how it is placed in the brain. In preclinical trials it seemed to allow relatively primitive communication with paralyzed patients. Even primitive communication can be a life-saver for people who are totally paralyzed. It also demonstrates the strides being made in technology that will directly connect human brains with the outside world. Are we on the way to "Resistance is futile?" [Borg reference from "Star Trek: A New Generation", to those much younger than I.] I don't think so, but an argument could be made. --- Hugh B. Wellons

---

Evolving Cybersecurity to Protect Today's Energy Network Architecture

"While the ramifications of a cyberattack on the energy sector could be extraordinary, energy companies face many of the same challenges as organizations in other verticals."

Why this is important: This article has a lot of good information about cybersecurity threats facing the energy sector. The best may be the discussion of the evolving cybersecurity landscape. The threats it discusses seem like they would apply to many industries (though energy companies are unique as they

are part of the nation's critical infrastructure). Cybersecurity vulnerabilities now are being exploited by threat actors over long periods of time as they gain access and remain in a network by reviewing and exfiltrating data other than a system's top security priorities. The result can be a larger set of compromised data and larger harm to the company, its employees, and its customers. Also, work-from-anywhere employees increase cybersecurity concerns. The result is a need to shift the way in which data is protected. The article advocates for zero trust network access that requires authentication before any person is permitted to access a network no matter where they are physically located. --- Nicholas P. Mooney II

Nanotechnology in Medicine: Regulatory Trends and Nanotechnology Utilized in New Enhanced Oil Recovery Method

"GlobalData expects the market to continue to grow until at least 2026, with regulatory bodies continuing to approve any repurposing of microbubbles for the delivery of therapeutic compounds adding to the momentum."

"This innovative approach has the potential to improve oil recovery, minimize costs of chemical agents, and eliminate alkali deposits and formation erosion."

Why this is important: Two articles on nanotechnology. The first provides a short summary of how various agencies govern nanotech medical products now. The overall answer seems to be, not as well as they should. Nanotechnology usually is thought of in terms of medical devices, but uses are being offered that apply the technology to internal and even pharmaceutical purposes. There is a special group at the FDA to deal with such crossover treatments, but parameters for handling this are difficult to design. This will be an ongoing struggle, because the possible uses are almost limitless. Assuring safety for such a wide array of uses is difficult.

The second article deals with using nanotechnology to improve the efficiency of oil recovery. It is an example of the wide array of uses. It is an interesting article, but I list it here primarily because it demonstrates the variety of uses for nanotechnology. --- Hugh B. Wellons

---

Improving Medical Device Security with Adversarial Thinking

"The best defense for a cybersecurity attack in medtech is a strong offense."

Why this is important: The alarm bells for cybersecurity in the medical device market are ringing. Are we listening to the data? Studies conducted over the past two years reveal harrowing details of the current state of cybersecurity in the United States. Noteworthy findings identified in this article include data showing a 700 percent increase in COVID-related phishing attacks, and 162 unique hacking incidents on healthcare entities that impacted more than 12.6 million individuals in just a three-month period. Other studies show that as many as 42 percent of hospital systems responded to a survey identified having experienced at least two ransomware attacks. And perhaps most alarming, researchers at Unit 42 (a strategic advisor in cybersecurity and incident response) found that as many as 75 percent of infusion pumps analyzed in their study still had known security gaps. This article proposes that manufacturers, practitioners, and patients should implement principles of adversarial thinking in developing strategies for improving (and preventing) cybersecurity vulnerabilities. The proposed five-step best practices model includes developing a threat mode, performing an exploits and impact analysis, implementing security risk controls, then verifying those controls, and preparing a security risk management report to include with FDA submissions. Fortunately, these same principles lay at the heart of what the PATCH Act is proposing to require for improving cybersecurity in medical devices. Essentially, manufacturers seeking approvals will need to lay out their plans for how they will go about monitoring for vulnerabilities and updating devices across the full life cycle. The insights in this article track well with what advocates and industry leaders are proposing and requesting. --- Brian H. Richardson

---

A Cashless Future: Can Big Data Change How We Pay?

"After Fintech proved to be the most successful evolving industry in 2021, it's no surprise that digitally active audiences are opting for new technology-infused transactions aids such as Paypal and Monzo."

Why this is important: A recent study suggested cash could quickly become extinct. The survey found an increasing number of people preferring to pay in a way other than cash. The lowest percentage was 33 percent in the Philippines, while South Korea had the largest percentage at 77 percent. The U.S. was somewhere in the middle at 58 percent. In addition to the individual country percentages, the study reported that 59 percent of people believe that cash will disappear by 2030. The article also discusses some of the reasons behind the growth of these percentages, and they'll sound familiar to readers of *Decoded*. The biggest one discussed was the COVID-19 pandemic, which forced people to engage in commerce in a way that they viewed as clean and safe. The article also discusses how big data can impact how customers shop. The ever-growing amount of data about every person can be used to access and then predict their transaction history and income changes. That data then can be used to influence their decisions with targeted offers of credit among other things. --- Nicholas P. Mooney II

Concerns for Future Gene Therapy Testing in Laboratory Mice

"Researchers have found that new sickle cell disease gene therapies depend on choosing the right laboratory mice."

Why this is important: Gene therapy can be influenced by the patients chosen. In other words, like a lot of science, success really is in the details. Preclinical work helps to prevent deadly mistakes. Gene therapy has faced a lot of challenges, including the tragic death of Jesse Gelsinger and the resulting drought of gene therapy research. In a lot of ways, we are many years behind where we could be in gene therapy research. Gene therapy may be critical to implementing developments in CRISPR and related technologies. We must learn how to do this correctly. --- Hugh B. Wellons

---