“CYBER-ING AROUND THE CHRISTMAS TREE”

Kennedys cybersecurity and privacy (US) year in review

December 2021

Kennedys

Kennedys cybersecurity and privacy (US) year in review
December 2021

Kennedys

Table of contents

Section | Page no

Contents

Introduction

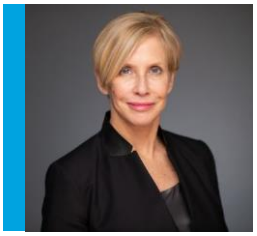
As the world emerged from lockdown, it should come as no surprise that cybersecurity and data privacy remained dominant topics in the media and legal industry. Some of 2021 was much like 2020 – ransomware attacks continued to fill the headlines, and in the aggregate, constituted significant loss paid under cyber insurance policies. OFAC reminded victim companies and incident response firms (and cyber carriers) that it remains unlawful to pay ransom payments to designated organizations. Comprehensive federal legislation addressing cyber defenses and notification requirements never materialized.

Yet in 2021, we saw new and very significant developments. US law continued its drift toward comprehensive privacy regulation with two new significant pieces of privacy legislation and California's enforcement of the California Consumer Privacy Act. In the absence of federal legislation, federal agencies either stepped up enforcement actions or signalled that they intend to do so within their realms of governance. Litigation under the Illinois Biometric Information Privacy Act continued its surge while the Illinois high courts rendered two impactful decisions and a Circuit court punted to Illinois's highest court. This review provides a brief synopsis of many of the events and developments that made our "list." Where available, we have linked this review to more in-depth articles written by Kennedys. We hope you enjoy.

Joshua Mooney

Partner

t +1 267 479 6706
e joshua.mooney@kennedyslaw.com



Judy Selby

Partner

t +1 646 625 3950
e judy.selby@kennedyslaw.com

Tracey Kline

Associate

t +1 267 479 6712
e tracey.kline@kennedyslaw.com

Alexis Childs

Pending admission

t +1 267 479 6734
e alexis.childs@kennedyslaw.com [1]

[1] The authors also wish to thank Bridget Mead and Javier Vijil for their work and contribution to the content of this year in review.

Kennedys

State Law Developments – privacy and breach notification

Data privacy

Perhaps one of the most significant developments in US privacy law for 2021 was the enactment of comprehensive data privacy laws in Virginia and Colorado. Both pieces of legislation, which go into effect in 2023, adopt frameworks resembling those in the EU General Data Protection Regulation 2016/679 (GDPR) and the California Consumer Privacy Act (CCPA). Both laws also grant consumers significant rights with respect to their personal data, but neither contains a private right of action.

The Virginia Consumer Data Protection Act (VCDPA),[2] which was signed into law on March 2, 2021 and becomes effective on January 1, 2023, established the following data subject rights for Virginia residents:

- Mandates responsibilities and privacy protection standards for data controllers and processors, with certain exceptions
- Grants consumers rights of access, accuracy, deletion, data portability, and allows consumers to opt-out of the processing of personal data for purposes of targeted advertising
- Requires "reasonably accessible, clear, and meaningful privacy notices" that disclose the categories of personal data processed and/or shared by the controller; the purpose for processing; how consumers may exercise their data subject rights; and the categories of third parties with whom controllers share personal data

[2] Va. Code Ann. § 59.1-575 *et seq.*

The law creates additional rights and requirements. The law defines "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person.

The Colorado Privacy Act (ColoPA), which was signed into law on July 7, 2021 and becomes effective on July 1, 2023, provides similar rights of access, correction, deletion, and portability over personal data.[3] Consumers also have the right to opt-out from the processing of their personal data for targeted advertising, sale of personal data, or profiling.[4] The law requires controllers that process personal data for targeted advertising or the sale of personal data to provide "a clear and conspicuous method to exercise the right to opt out."[5]

ColoPA also imposes on a controller the duties of transparency, specified purpose, data minimization, avoidance of secondary use, care, anti-discrimination, and consent when using sensitive data.[6] Furthermore, the law requires controllers employing third parties to enter into data processing agreements that have mandatory contractual provisions, including: (i) detailed processing instructions, including the nature and purpose of the processing; (ii) identification of the types of personal data to be processed and the duration of such processing; and (iii) duties of confidentiality.[7] Unlike CCPA and VCPA, the law applies to non-profits.

Breach Notification

On the data breach notification front, four states - Connecticut, Mississippi, Nevada, and Texas - enacted changes to their breach notification laws. The most significant changes imposed are as follows:

- Connecticut expanded the definition for "personal information" to include such data as individual taxpayer identification numbers, passport, military identification, and other government-issued ID numbers, medical information, and biometric data. The amended statute also shortens notice deadlines[8]
- Mississippi expanded the definition for "personal information" to include tribal identification card numbers[9]
- Nevada increased the severity of penalties by expanding the state's Deceptive Trade Practices Act to include violations of the data breach notification law as a deceptive trade practice. [10] Now businesses

[3] 6-1-1306.(1)(b) – (e).
[4] 6-1-1306.(1)(a).
[5] 6-1-1306.(1)(a)(III).
[6] 6-1-1308.
[7] 6-1-1305.(5).
[8] Conn. Gen. Stat. § 36a-701b.
[9] Miss. Code § 75-24-29.
[10] N.R.S. § 603A.010 *et seq.*

potentially may be liable under both the data breach notification law and the Deceptive Trade Practices Act.

- Texas now requires companies to provide additional information to the Texas Attorney General after discovery of a breach. The amended law also requires the Texas Attorney General to post online a listing of the notifications received for public access and to update and maintain the listing, as necessary.[11]

[11] Tex. Bus. & Com. Code § 521.053.

Biometrics privacy law

A New, New York Law

Significant developments took place in US biometric data law. On July 9, 2021, New York City's Biometric Identifier Law went into effect.[12] The law prohibits the sale or exchange "for anything of value" of "biometric identifier information," and requires "commercial establishments" that collect or store biometric identifier information to provide notice. Such notice must be "clear and conspicuous," written in "in plain, simple language," and located at the establishment's entrance.

The statute creates a private right of action with a cure provision for the signage requirement only. The law directs the NYC Commissioner of Consumer and Worker Protection to promulgate further guidance and regulations detailing additional requirements.

BIPA

2021 saw several consequential decisions involving the Illinois Biometric Information Privacy Act (BIPA).[13] Perhaps most significantly, on May 20, 2021, the Illinois Supreme Court issued a long-awaited ruling in *West Bend Mutual Insurance Company v. Krishna Schaumburg Tan, Inc.*[14] In that case, the court held that the undefined term "publication" in the context of a CGL policy's coverage for "publication of material that violates a person's right of privacy" means *both* the dissemination of information to the public at large *and*

[12] L.L. 2021/003, 1/10/2021, eff. 7/9/2021.
[13] 740 ILCS 14/1 *et seq.*
[14] *West Bend Mutual Insurance Company v. Krishna Schaumburg Tan, Inc.*, No. 125978, 2021 IL 125978 (Ill. May 20, 2021).

dissemination of information to a single party. The *West Bend* court further held that a distribution of material exclusion in the at-issue general liability policy did not apply to BIPA lawsuits.

On September 24, 2021, in *Massachusetts Bay Insurance Co. v. Impact Fulfillment Services, LLC*,[15] a North Carolina federal district court, applying North Carolina law, held that a different *and more recent* distribution of material exclusion—which was broader than the exclusion at issue in *West Bend*—barred coverage for an underlying BIPA lawsuit. While policyholder attorneys cheered the Illinois Supreme Court's decision in *West Bend*, the decision in *Massachusetts Bay* suggests that the question of whether the more recent and commonly used distribution of material exclusion at issue in *Massachusetts Bay* prohibits coverage for IPA is wide open. (As an aside, we note that whether the employment practices exclusion and the unauthorized access or disclosure of personal information exclusion prohibit coverage for BIPA claims remains undecided under Illinois law.)

Meanwhile, an Illinois appellate court finally provided an answer to the open question of what statute of limitations applies to BIPA claims. On September 17, 2021, in *Tims v. Black Horse Carriers, Inc.*,[16] the Appellate Court of Illinois for the First District held that actions under section 15(c) and (d) of BIPA are governed by a one-year statute of limitations, while actions under section 15(a), (b), and (e) of the act are governed by a five-year statute of limitations.

Briefly, the defendant Black Horse moved to dismiss several BIPA claims on the ground that Illinois's one-year limitation period for "[a]ctions for slander, libel or for publication of matter violating the right of privacy" applied. Black Horse argued that the one-year limitation applied to all BIPA claims because BIPA is a privacy protection statute. The appellate court analyzed the scope of the one-year statute of limitation under section 13-201 of the Illinois Code. Focusing on the statute's express language, which stated that it applied to actions "for publication of matter violating the right of privacy," the court concluded that the limitations period did not apply to all privacy actions, but instead applied only to those actions where "*publication is an element or inherent part of the action*" (emphasis added).

Thereafter, looking to the causes of actions under BIPA, the court concluded that "at least three of them have *absolutely no element of publication or dissemination*" (emphasis added), namely sections 15(a), 15(b), and 15(e), and therefore the one-year statute of limitation did not apply to them:

> A private party would violate section 15(a) by failing to develop a written policy establishing a retention schedule and destruction guidelines, section 15(b) by collecting or obtaining biometric data without written notice and release, or

[15] *Massachusetts Bay Insurance Co. v. Impact Fulfillment Services, LLC*, No. 1:20CV926, 2021 WL 4392061 (M.D.N.C. Sept. 24, 2021).
[16] *Tims v. Black Horse Carriers, Inc.*, No. 1-20-0563, 2021 IL App (1st) 200563 (Ill. App. Ct. 1st Dist. Sept. 17, 2021).

> section 15(e) by not taking reasonable care in storing, transmitting, and protecting biometric data. Id. § 15(a), (b), (e).

According to the court, a plaintiff could commence a BIPA lawsuit alleging violation of section 15(a), (b), and/or (e) without having to allege or prove a disclosure or dissemination of any biometric data. "Stated another way, an action under section 15(a), (b), or (e) of the Act is *not* an action 'for publication of matter violating the right of privacy.'" (Emphasis added.) On the other hand, the court held that sections 15(c) and (d) required a publication or disclosure of biometric data as one of the elements necessary to establish liability. Thus, the court concluded that "an action under section 15(c) or (d) is an action 'for publication of matter violating the right of privacy,'" thereby implicating the one-year statute of limitation under section 13-201 for "[a]ctions for slander, libel or for publication of matter violating the right of privacy." This explanation may have a significant impact on coverage litigation.

The *Tims* decision is currently the highest Illinois state court opinion on the issue of what limitations period(s) governs BIPA claims. However, the decision will likely be appealed to the Illinois Supreme Court. Moreover, it may not be the last word by an Illinois appellate court on the issue; the Third District of the Illinois Appellate Court has a BIPA statute of limitations appeal pending before it in *Marion v. Ring Container Technologies, LLC*.[17]

In *Cothron v. White Castle System, Inc.*, the Seventh Circuit was to decide whether, when conduct that allegedly violates BIPA is repeated, a BIPA claim accrues only once, upon the first instance of a violation, or if, instead, a BIPA claim accrues each time a violation occurs. Sneaking in just before we went to press, in a December 20, 2021 decision, the Seventh Circuit certified the question to the Supreme Court of Illinois.[18]

In *Cothron*, the plaintiff, an employee of defendant White Castle System, Inc. alleged that White Castle unlawfully had collected scans of her fingerprints and unlawfully had disclosed them to its third-party vendor in violation of sections 15(b) and 15(d) of BIPA. White Castle filed a motion for judgment on the pleadings based on the statute of limitations, alleging that the plaintiff's suit was untimely because a claim under BIPA accrued the first time Cothron scanned her fingerprint into White Castle's system after BIPA took effect in 2008. Because that occurred more than a decade before the plaintiff sued, White Castle contended that the plaintiff's suit was untimely under the longest possible limitations period. Cothron responded that every unauthorized fingerprint scan amounted to a separate violation of BIPA, so a new claim accrued with each scan and her suit was therefore timely for the scans within the limitations period.

The district court rejected White Castle's "one time only" theory of claim accrual, but found the question close enough to warrant an interlocutory appeal. Cothron asked the US Court of Appeals for the Seventh Circuit to certify

[17] *Marion v. Ring Container Technologies, LLC*, No. 3-20-0184 (Ill. App. Ct. 3d Dist.).
[18] *Cothron v. White Castle System, Inc.*, No. 20-3202, 2021 WL 5998537 (7th Cir. Dec. 20, 2021)

the question to the Illinois Supreme Court. The Seventh Circuit agreed that the issue was best suited for Illinois's highest court. Accordingly, the Seventh Circuit certified the following question to the Illinois Supreme Court: "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?"

Finally, the issue of whether BIPA statutory damages claims brought by employees against their employers are preempted by the Illinois Workers' Compensation Act remains pending before the Illinois Supreme Court in *McDonald v. Symphony Bronzeville Park, LLC*.[19]

[19] *McDonald v. Symphony Bronzeville Park, LLC*, No. 126511 (Ill.).

CPRA and CCPA enforcement actions

The California Office of Attorney General (OAG) was hard at work this year enforcing the California Consumer Privacy Act (CCPA). After just one year after CCPA officially took effect, the OAG commenced several enforcement actions that have highlighted a low tolerance for non-compliance with the most rudimentary requirements of CCPA. Further, to spotlight key areas of the its focus for CCPA enforcement, the OAG published CCPA Enforcement Case Examples, which provides multiple illustrations of how businesses failed to comply with CCPA. Although the illustrations cover a wide range of topics, we discussed several OAG enforcement actions concerning notice requirements, privacy policies, and service provider contracts here.

Meanwhile, on December 16, 2020, the first provisions of the California Privacy Rights Act (CPRA) creating the California Privacy Protection Agency (CPPA) took effect. (Most provisions become effective on January 1, 2023.) The CPPA will assume rulemaking responsibilities from the OAG by July 1, 2021, and must adopt final privacy regulations by July 1, 2022.

In addition, provisions extending the business-to-business and employee exemptions under CCPA until January 1, 2023, the date on which the CPRA becomes fully operative, have gone into effect.[20] Reportedly, the two-year period is intended to allow lawmakers additional time to pass legislation to extend these exemptions.

[20] Cal. Civ. Code § 1798.145(m) and (n).

Federal developments

The Securities and Exchange Commission

The SEC ramped up its cybersecurity enforcement, filing several administrative orders that signal increased scrutiny of both cyber-related disclosures and compliance with the Safeguards Rule.

- In *In the Matter of Pearson PLC,* Pearson filed a Form 6-K stating that the risk of a data privacy incident or failure to comply with data privacy regulations *could* result in a major data privacy or confidentiality breach. The statement was identical to prior Form 6-K disclosures and did not identify that Pearson in fact had a major data privacy breach. Determining that the statement was misleading, the SEC found that Pearson had violated Section 17 of the Securities Act, requiring accurate and true statements of material facts in reporting, and Section 13 of the Exchange Act, requiring disclosure controls and procedures. Pearson was fined $1 million.
- *In the Matter of First American Financial Corporation* focused on alleged disclosure deficiencies related to internal disclosure controls, which included failing to inform its CISO, CIO and Board of Directors of a known vulnerability. The SEC fined First American $487,616 for violating Rule 13 of the Exchange Act, citing the senior executives' lack of knowledge of the discovery of the vulnerability and the company's statements claiming that they "took immediate action to address the situation" deficiencies in disclosure controls.

The agency also commenced several enforcement actions for violation of the SEC's Safeguards Rule, which requires covered organizations to adopt written policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information,[21] including:

- *In the Matter of Cetera Advisor of Networks, LLC, et al.*, involved companies' failure to fully implement multi-factor authentication safeguards and misleading timelines in notification letters to consumers impacted by cybersecurity incidents.
- *In the Matter of Cambridge Investment Research, Inc., et al.*, involved the failure to implement firm-wide enhanced security measures, including MFA, for several years after a cybersecurity incident involving email account takeovers.

The SEC's actions in 2021 show that having a written cybersecurity program is not enough. Companies need to ensure that they are effectively implemented, including internal reporting with an involvement of senior management, changes to programs to mitigate discovered vulnerabilities, and employee training.

The US Department of Treasury Office of Foreign Assets Control (OFAC)

In September, OFAC issued an "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." Under the International Emergency Economic Powers Act (IEEPA)[22] and the Trading with the Enemy Act (TWEA),[23] persons in the US and US corporations are prohibited from engaging in transactions, directly or indirectly, with individuals or entities placed on the Specially Designated Nationals and Blocked Persons List (SDN List) promulgated by OFAC, and/or those with those persons or organizations covered by comprehensive country or region embargoes (for example, Cuba, Iran, and North Korea). Persons and organizations included on OFAC's SDN List may be found here: https://sanctionssearch.ofac.treas.gov/. Violation of IEEPA carries a civil fine of either $250,000 (USD) or an amount *twice* the amount of the ransom paid to threat actors.[24] Civil liability may be established based on strict liability, "meaning that a person subject to US jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC."[25] Violation of

[21] *See* 17 CFR § 248.30.

[22] 50 U.S.C. §§ 1701–06
[23] 50 U.S.C. §§ 4301–41
[24] 50 USC § 1705(b).
[25] September 2021 OFAC Guidance at 4.

IEEPA also carries criminal liability a $1 million fine, 20 years imprisonment, or both.[26] Violation of TWEA likewise carries with it criminal liability in the form of a $1 million fine, 20 years imprisonment, or both.[27]

The OFAC guidance reiterated these prohibitions and mitigating factors the agency would consider if a person or organization were prosecuted. Mitigating factors include undertaking "meaningful steps" to reduce the risk of extortion by a sanctioned actor by adopting or improving cybersecurity practices. Identified safeguards include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating anti-virus and anti-malware software, and employing authentication protocols. Another significant mitigating factor is cooperation with law enforcement, including timely and voluntary reporting of ransomware attacks to law enforcement.

The guidance also reiterated the ability to submit applications to OFAC to permit an otherwise prohibited ransom payment, which are reviewed on a case-by-case basis with a presumption of denial. (A note: as of the writing of this article, the authors are unaware of any license application approved by OFAC.)

The United States Department of Justice (DOJ)

In October, DOJ announced the launch of its Civil Cyber-Fraud Initiative to pursue government contractors that knowingly misrepresent their cybersecurity safeguards or fail to monitor and report cybersecurity incidents. Led by the Civil Division's Commercial Litigation Branch, Fraud Section, DOJ attorneys will employ the False Claims Act (FCA) to bring claims against contractors that:

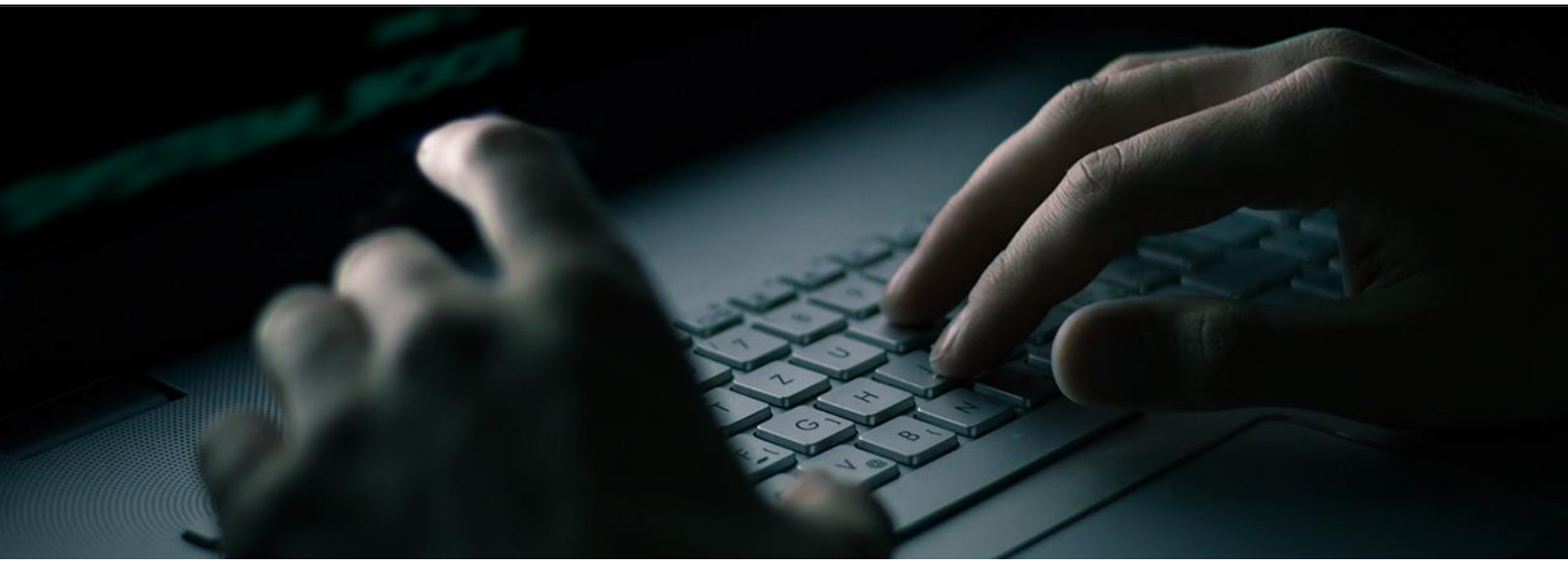
- Knowingly provide deficient cybersecurity products or services
- Knowingly misrepresent their cybersecurity practices or safeguards or
- Knowingly violate obligations to monitor and report cybersecurity incidents and breaches

[26] 50 USC § 1705(c).
[27] 50 USC § 4315(a), (b)(1).

The Federal Trade Commission

In November, the FTC released its update of Standards for Safeguarding Customer Information to the Safeguards Rule.[28] Acknowledging that many businesses that collect and process sensitive consumer data may not be covered by the Rule, changes to the Rule expanded the definition for "financial institution" to include entities engaged in activities deemed by the Federal Reserve Board to be "incidental" to financial activities. New requirements also have some similar themes in light of the SEC's enforcement actions. Companies should undertake written risk assessments to identify vulnerabilities, and implement specific safeguards to address them, including internal access controls, use of MFA, implementation of effective employee training, and establishment of internal reporting and accountability processes with senior management and, where applicable, boards of directors. The rule, however, provides some exemptions for organizations that collect and process data of fewer than 5,000 consumers.

[28] 16 CFR Part 314: Standards for Safeguarding Customer Information (Final Rule), available at https://www.ftc.gov/system/files/documents/federal_register_notices/2021/10/safeguards_rule_final.pdf.



Silent cyber coverage

2021 was the year for policyholder-friendly silent cyber coverage decisions. In addition to *West Bend*, discussed above, three other notable decisions made our list. One of the most concerning silent cyber cases of the year was the Fifth Circuit's decision in *Landry's Inc. v. The Insurance Co. of the State of Pennsylvania*.[29] There, the court held that a CGL insurer had a duty to defend under Coverage B, personal and advertising injury coverage, for a claim arising out of a third party data breach.

The insured had been sued by its payment card processing vendor for costs related to a breach of credit card data from the insured's point-of-sale system. The breach resulted in unauthorized charges to some consumers' credit cards. Under its agreements with Visa and MasterCard, the vendor was assessed over $20 million in fines and losses related to the breach. The vendor looked to recover those costs from the insured, claiming that the insured breached its contractual cybersecurity obligations to the vendor. When the insured refused to indemnify, the vendor filed suit, and the insured sought coverage under CGL Coverage B for "personal and advertising injury."

The policy defined "personal and advertising injury" in part as an "injury ... arising out of one or more of the following offenses":

> (d) Oral or written publication, in any manner, of material that slanders or libels a person or organization;
>
> (e) Oral or written publication, in any manner, of material that violates a person's right of privacy.

[29] *Landry's Inc. v. Ins. Co. of State of Pa.*, 4 F.4th 366 (5th Cir. 2021).

In the subsequent coverage litigation, the Texas federal district court granted summary judgment for the insurer, holding there was no alleged "personal and advertising injury," but the Fifth Circuit reversed. The Court of Appeals first held that "publication, in any manner," meant that "the Policy intended to use every definition of the word 'publication' – even the very broadest ones." Based on that observation, the court concluded that "even merely 'exposing or presenting [information] to view'" satisfied "the Policy's capacious provision." The court also ruled that because "oral or written publication, in any manner" appeared in both the offenses for defamation and privacy, the term must have the same meaning – i.e., applying the publication standard for a defamation to a privacy claim. (Note, they are not even remotely the same.)

In addition, the court rejected the insurer's argument that the claim was not covered because it arose from the insured's alleged breach of contract, and not a violation of privacy rights. Focusing on the phrase "arising out of," the court held that the policy "does not simply extend to violation of privacy rights; the Policy instead extends to all injuries that arise out of such violations." Consequently, the court ruled that the insurer had a duty to defend.

Although some have argued that this decision signals a broadening of coverage for data breaches, we believe the decision should have a limited impact. For one, the policy did not have the "access or disclosure of confidential or personal information and data-related liability" exclusion that CGL policies routinely have today. In addition, while the court provided a broad interpretation for the phrase "publication, in any manner," many more courts have explicitly rejected such a reading. The *Landry* court also conflated the insured's alleged breach of contract – which should have triggered the breach of contract exclusion – with the affirmative act of publication. The insured did not publish, share or disseminate anything.

In *G&G Oil Co. of Indiana, Inc. v. Continental Western Ins. Co.*,[30] the Indiana Supreme Court reversed an appellate court's ruling that a ransom payment did not implicate coverage under a commercial crime section of a multi-peril policy. The insured, victimized by a ransomware attack it suspected had resulted from targeted spear-phishing email, sought coverage under a Computer Fraud insuring agreement. The provision stated:

> We will pay for loss or damage to "money", "securities" and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the "premises" or "banking premises" … **a.** To a person … outside those "premises" …

The insurer denied coverage, and in the subsequent coverage litigation, the trial court found that the loss was not "fraudulently caused," but was instead the result of theft. The court also determined that the payment did not qualify as a loss "resulting directly from the use of a computer," but instead "was a voluntary payment

[30] *G&G Oil Co. of Ind. v. Continental Western*, 165 N.E.3d 82 (Ind. 2021).

to accomplish a necessary result." The Indiana Court of Appeals affirmed unanimously. The Indiana Supreme Court reversed.

The insured argued that the "resulted directly from the use of a computer" requirement had been satisfied because a computer was part of the entire ransomware scheme. The court agreed, stating that the loss had resulted either immediately or proximately from the use of a computer because the insured's "transfer of Bitcoin was nearly the immediate result—without significant deviation—from the use of a computer." The court also disagreed that the ransom payment had been voluntary. The court stated that "the payment more closely resembled one made under duress," and that it "was not so remote that it broke the causal chain." The court further determined that the phrase "fraudulently cause a transfer" had been interpreted too narrowly by the lower court, concluding that the phrase "can be reasonably understood as simply 'to obtain by trick'." The court then remanded the case for a factual determination with respect to that issue.

In our view, the court got two crucial issues wrong. First, even under the "caused by trick" definition of fraud, the only potential trickery involved the suspected spear-phishing email. It is beyond dispute that the insured made a clear eyed transfer of funds to the criminal hacker and was under no illusion that it was anything other than a ransom payment. Second, the court inexplicably introduced the concept of duress into the "fraudulently cause a transfer" requirement. Duress and fraud are not the same thing; a knowing transfer made under duress is not a fraudulently caused transfer. For these reasons, we do not expect the reasoning of the court in *G&G Oil* to be followed by courts outside of Indiana.

Finally, and very recently, we have the decision *EMOI Services, LLC v. Owners Insurance Co.* rendered by the Ohio appellate court.[31] There, the insured sought coverage under the Electronic Equipment Endorsement in the property section of its business owner's policy for costs to restore data following a ransomware attack. The Endorsement provided:

> When a limit of insurance is shown in the Declarations under ELECTRONIC EQUIPMENT, MEDIA, we will pay for direct physical loss of or damage to "media" which you own, which is leased or rented to you or which is in your care, custody or control while located at the premises described in the Declarations. We will pay for your costs to research, replace or restore information on "media" which has incurred direct physical loss or damage by a Covered Cause of Loss.
>
> Direct physical loss of or damage to Covered Property must be caused by a Covered Cause of Loss.

[31] *EMOI Servs., LLC v. Owners Ins.*, No. 29128, 2021 WL 5144828 (Ohio Ct. App. Nov. 5. 2021).

The Endorsement defined "media" as "materials on which information is recorded such as film, magnetic tape, paper tape, disks, drums, and cards," and included electronic data stored on such media.

The insurer argued that there was no coverage because "[n]o film, magnetic tape, disc, drum, card, etc., has been identified as ***physically*** damaged in [the] claim" (emphasis in original). The court rejected that argument, stating:

> We do not find it reasonable to interpret the phrase [covered media] to mean only media that has incurred a covered loss, as [the insurer] suggests. In this case, because the computer software and reproduction of data was contained on [the insured's] servers, i.e., "covered media", those items also met the definition of media.
>
> [The insurer's] reading of the definitional section renders meaningless the sentence defining media to include "software and reproduction of data on covered media." Without that sentence, the definition of media reasonably would be restricted to tangible electronic storage media, and the policy already includes a provision stating "We will pay for your costs to research, replace or restore information on 'media' which has incurred direct physical loss or damage by a Covered Cause of Loss."

Accordingly, the court also held that "the policy contemplated that [the insured's] software and reproduction of data was capable of being physically damaged." Although the insured was able to access its files after the decryption program was run, the insured's expert testified that some programs remained unusable. Construing that evidence in the insured's favor, the court held that "the evidence supports a conclusion that the encryption damaged [the insured's] software and data." Finding that this evidence raised material issues of fact concerning whether the software was damaged, the court remanded the case to the trial court. Troublingly, the court also found that there were issues of fact concerning whether the insurer handled the claim in good faith.

What is so troubling is that the court's decision to remand seems to be based on the concept that encrypting data by adding an extension to media files constitutes *physical* damage. (We note that even the insured's own expert agreed that "once you get the code, you can unlock it to read it or use the information that's being sent.") If a door is locked, is the doorway physically damaged? The *EMOI* court apparently thinks so. The dissent focused on the threshold coverage issue of no physical loss or damage to media, and we think the dissent got it right. Notably, the dissent also disagreed that there were factual issues concerning the insured's bad faith claim; since the insurer "made the correct coverage call, its refusal to pay [the] claim was 'predicated upon circumstances that furnished reasonable justification' for the refusal." If an appellate judge believes the insurer's denial was correct, how can the denial match the legal standard for bad faith?

Further adoption of NAIC's model law for insurance data security

The Insurance Data Security Model Law, issued by the National Association of Insurance Commissioners (NAIC) in 2017, made its way into seven more states in 2021. The Model Law (MDL-668) establishes data security standards for regulators and insurers in order to mitigate the potential damage of a data breach[32] and requires insurers and other entities licensed by the state department of insurance to develop, implement, and maintain an information security program based on risk assessment.[33]

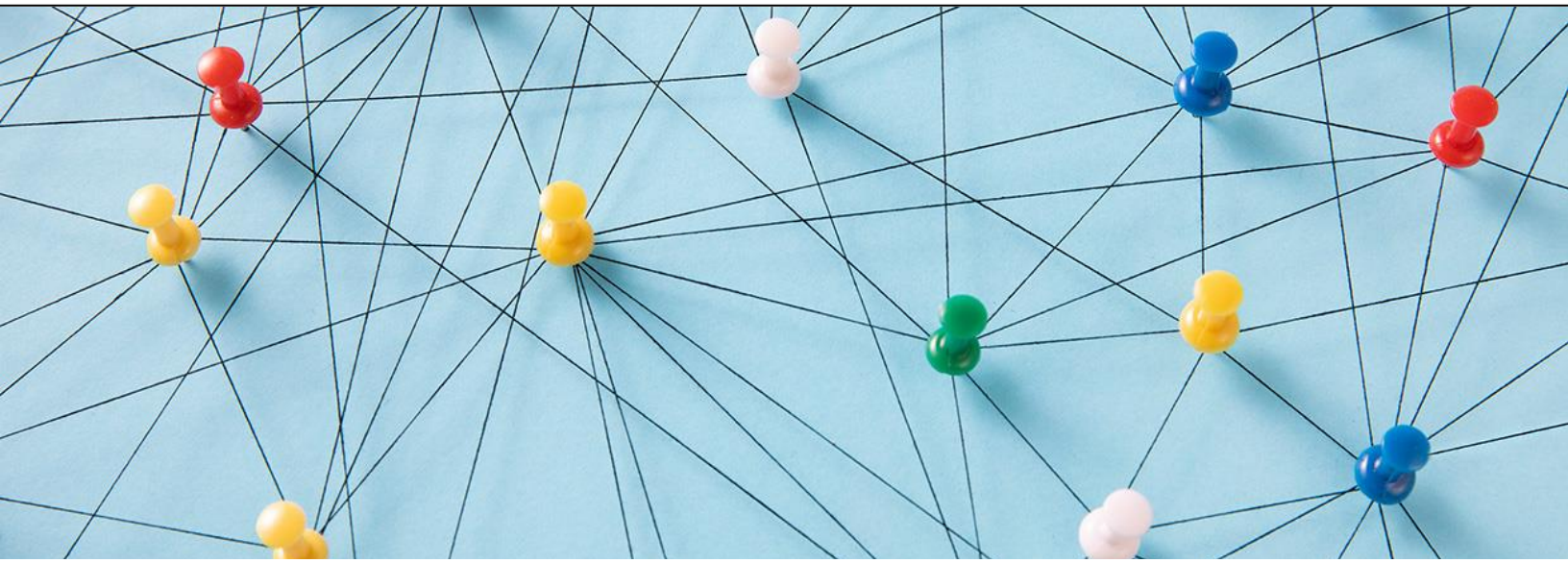
The seven states to adopt their version of the Model Law in 2021 were Hawaii (S.B. 1100), Iowa (H.F. 719), Maine (H.P. 17), Minnesota (HF 6, Article 3, Section 5), North Dakota (S.B. 2075), Tennessee (HB 766), and Wisconsin (SB 160), bringing the total number of states with similar laws to 19.[34]

---

[32] *See* Holly Weatherford, Jennifer McAdam, and Chara Bradstreet, State Legislative Brief, The NAIC Insurance Data Security Model Law (June 2020).

[33] *Id.*

[34]Alabama (Ala. Code §§ 27-62-1 to 27-62-11); Connecticut (HB 7424); Delaware (18 Del. C. §§ 8601 to 8611); Hawaii (SB 1100); Indiana (Ind. Code §§ 27-2-27-1 to 27-2-27-32); Iowa (H.F. 719); Louisiana (HB 614); Maine (H.P. 17); Michigan (MCL 500.550 to 500.565); Minnesota (HF 6, Article 3, Section 5); Mississippi (Miss. Code Ann. §§ 83-5-801 to 83-5-825); New Hampshire (N.H. RSA § 420-P:1 to 14); New York (23 NYCRR 500.0 to 500.23) (note that the NAIC Model Law was modelled after this NYDFS cyber regulation); North Dakota (SB 2075); Ohio (Ohio R.C. 3965.01 to 3965.11); South Carolina (S.C. Code Ann. § 38-99-10 to 38-99-100); Tennessee (HB 766); Virginia (Va. Code Ann. §§ 38.2-621 to 38.2-629); Wisconsin (SB 160).



Some international developments

The PRC's Personal Information Protection Law

The People's Republic of China (PRC) jumped aboard the data privacy train in 2020. On August 20, 2021, the PRC enacted the Personal Information Protection Law (PIPL), which took effect on November 1, 2021. The PIPL serves as the regulatory model for personal information in its jurisdiction. Some highlights:

- Under Article 4, PIPL broadly defines personal information as data "related to identified or identifiable natural persons recorded by electronic or other means."
- Article 28 defines "sensitive personal information," which carries heightened processing requirements, as personal information that can "easily" lead to the infringement of a data subject's dignity or harm of his or her safety or property if such data is leaked or used lawfully." Examples of sensitive information include biometrics, religious belief, specific identities, medical health, financial accounts, whereabouts, and the personal information of minors under the age of 14.
- Like GDPR, in order to process personal information, a company must have a legal basis, which are listed under Article 13.
- Consent must be voluntary and explicit, and given with full knowledge
- Under Article 40, both critical information infrastructure operators (CIIOs) and organizations that process a certain threshold of personal information exceeding an amount determined by the Cyber Administration of China (CAC) must locally store in China the personal information they collect and generate in China, and pass a CAC security assessment.
- Under Article 17, before a company may process personal information, it must "truthfully, accurately, and completely" inform the data subject, "in an eye-catching manner and with clear and understandable language" (i) the processor's contact information; (ii) the purpose and method of

processing; (iii) the type of personal information processed; (iv) the retention period of the personal information processed; and (v) the method and procedure by which data subjects may exercise their rights.

Under Article 3, PIPL purports to have broad extraterritorial reach, applying to processing activities engaged outside of the PRC of personal information of data subjects located in the PRC where: (i) the purpose is to provide products or services to data subjects in the PRC; (ii) the purpose is to analyze and evaluate the activities of data subjects in the PRC; or (iii) other circumstances provided by laws and administrative regulations. Businesses can face fines of 50 million RMB (about $7.7 million USD) or 5% of an entity's worldwide revenue from the prior fiscal year for violations. Read more about it here.

The EU's New Standard Contractual Clauses

Out with the old and in with the new (unless you are in the UK)! The European Commission released a new set of Standard Contractual Clauses, which were approved by EU Decision C2021/3972, issued on June 4, 2021. The new Standard Contractual Clauses still require the recipient to provide the personal data with most of the same protections required under the GDPR, but should be simpler to use and understand because they more closely reflect the requirements of the GDPR. (The old Standard Contractual Clauses were drafted to reflect the Directive.) Use of the new SCCs for all new contracts—*and* new processing activities—became mandatory as of **September 27, 2021**. Organizations must amend all existing contracts that use the old SCCs and were entered into before September 27, 2021, to the new SCCs by **December 27, 2022.**

Perhaps the biggest change is that the new SCCs now offer four potentially applicable modules: (1) a controller to another controller, (2) from a controller to a processor, (3) from a processor to sub-processor, or (4) from a processor to a controller. Furthermore, the new SCCs also have a docking clause to permit new parties to join the contract. The new SCCs also have an Article 28 processor clause, so no additional data processing agreements are needed with processors.

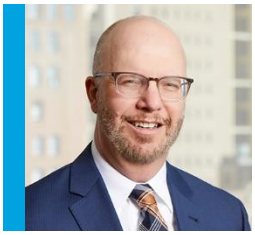
Note that the new SCCs do not apply in the UK. Therefore, transfers of personal data outside of the UK to a country that does not have an adequacy decision must employ the old SCCS. In addition, to comply with the *Schrems II* decision, the new SCCs may need to be accompanied by supplementary measures to ensure appropriate levels of protection for transferred data.

Panama's Breach Notification Law

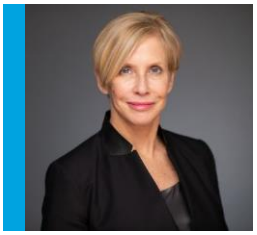
In March 2021, Panama enacted its first privacy and data protection law, Law No. 81 on Personal Data Protection (the 'Law") which is regulated by Executive Decree No. 285 (the Decree). The Law adopts GDPR-like protections. Article 2 requires handlers of personal data to implement technical and organizational processes to safeguard personal data. Article 5 establishes that the Law applies to databases that are located within Panamanian territory and data handlers who reside in Panama. Article 2 further explains that in the event of a breach, data handlers are obliged to provide notice to the data owner. The notification of data breach must be delivered to the regulator and the owner "within 72 hours of when the incident was discovered and should contain clear language."

As with any other rule, the Law does address non-compliance. Chapter VI sets forth three categories of noncompliance: minor, grave, and very grave. Depending on the category that the violation falls within, the sanctions that the National Authority of Transparency can impose range from appearances before the ANTAI (minor infraction) to fines anywhere between USD $1000.00 to USD $10,000.00 (grave infraction) to the permanent closing or suspension of the activities of the data holder (very grave infraction).

Key contacts

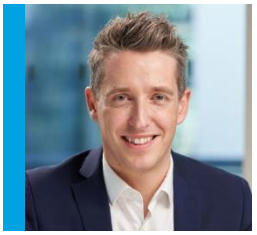


Joshua Mooney
Partner, US
t +1 267 479 6706
e joshua.mooney@kennedyslaw.com



Judy Selby
Partner, US
t +1 646 625 3950
e judy.selby@kennedyslaw.com

Oliver Dent
Partner, UK
t +44 161 829 7462
e oliver.dent@kennedyslaw.com



Tom Pelham
Partner, UK
t +44 161 829 7453
e tom.pelham@kennedyslaw.com

Joanie Ko
Partner, APAC
t +852 2848 6318
e joanie.ko@kennedyslaw.com

Nicholas Blackmore
Special Counsel, APAC
t +61 3 9498 6602
e nicholas.blackmore@kennedyslaw.com

Kennedys

Kennedys

KennedysLaw

kennedyslaw.com