RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY

Mailise R. Marks, Daniel Cotter, Ariane Janz, Kenneth Williams, and Anthony E. Sinapi[*]

[*] *Ken Williams is a Shareholder and Mailise Marks is an Associate at Segal McCambridge Singer & Mahoney. Daniel Cotter is a Partner at Howard & Howard Attorneys PLLC. Ariane Janz is an Associate at Gordon Rees Scully Mansukhani, LLP. Anthony Sinapi is Of Counsel at Sinapi Law Associates, Ltd.*

This survey reviews recent statutory developments and court decisions in the area of cybersecurity and data privacy law from October 1, 2019, through September 30, 2020. The first part discusses significant state data privacy and security statutes that were enacted, became effective, or are the most significant to practitioners during the survey period. The second part discusses significant court decisions exploring insurance coverage for silent cyber coverage, biometric privacy, and the right to privacy.

I. STATUTORY IMPROVEMENTS IN CONSUMER AND DATA BREACH NOTIFICATION LAWS

All fifty states and most of the territories in the United States have enacted data-breach notification laws. Due to disruptions caused by the COVID-19 pandemic, much of 2020 has been spent working remotely. This shift to remote work led to the California Consumer Privacy Act and the New York SHIELD Act's enforcement provisions to come front and center as the Zoom application replaced the conference room. Additionally, data-breach notification statutes came into effect, giving residents additional protections by way of including more categories of "personal information" such as the inclusion of tax identification numbers and greater protection over medical records. The amendments also tended to provide more transparency to consumers and Attorney Generals' Offices by increasing the amount of information in the notices issued.

A. *National Enforcement Examples from the California Consumer Privacy Act, the New York "SHIELD" Act, and Zoom*

The new decade brought with it many new twists and turns in the field of data privacy and cyber security. While the California Consumer Privacy Act (CCPA)[1] and New York's "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act)[2] were much discussed at the outset of 2020 as formidable enforcement and investigation tools, no one could have anticipated that these two pieces of legislation would be tested so quickly by a little known video conference program known as Zoom.[3] On January 1, 2020, the majority of the CCPA went into effect, including the private

1. *See* Cal. Civ. Code §§ 1798.100–1798.199.
2. *See* N.Y. Gen. Bus. Law §§ 899-aa, 899-bb.
3. Zoom refers to Zoom Video Communications, Inc.

right of action and the enforcement action provisions.[4] The SHIELD Act went into force several months later on March 21, 2020.

Zoom is a video conference platform that became ubiquitous in homes across the United States as the COVID-19 pandemic required many companies to institute remote work policies intended to slow the spread of the virus. However, Zoom's surge in usage and popularity brought scrutiny from the New York Attorney General's Office under the SHIELD Act and with private actions asserted in California under the CCPA. The issue was simple: for all its convenience, the program had a lackluster cybersecurity system. The most obvious issue was so-called "zoom-bombing"—hackers entering purportedly private video conference rooms and engaging in offensive behaviors.[5]

In New York, the Attorney General's office issued a letter to Zoom's offices, which, according to the *New York Times*, requested information regarding the measures Zoom had implemented to protect the increased traffic and to detect hackers.[6] Further, the letter purportedly expressed numerous concerns with security flaws that permitted "malicious third-parties" to "surreptitiously access consumer webcams."[7] The Attorney General further sought more information about "whether Zoom has undertaken a broader review of its security practices."[8] The letter also referenced contemporaneous reports of Zoom sharing user data with other entities like Facebook and requested that Zoom provide information regarding the categories of data that it collected from users.[9] On May 7, 2020, Zoom and the New York Attorney General's Office came to a Letter Agreement that provided:

> Zoom shall comply with Executive Law § 63(12) and GBL §§ 349 and 350, and shall not misrepresent the collection . . . and safeguarding of consumers' personal information and regulation of abusive activity on its platform. . . . Zoom shall comply with the Children's Online Privacy Protection Act ("COPPA") Rule, 16 C.F.R. Part 312. . . . Zoom shall comply with New York Education Law § 2-d and implementing regulations, 8 N.Y.C.R.R. Part 121, and related regulations.[10]

4. *See* Cal. Civ. Code §§ 1798.150, 1798.155(b).

5. Kristen Setera, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FBI Boston (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

6. Danny Hakim & Natasha Singer, *New York Attorney General Looks into Zoom's Privacy Practices*, N.Y. Times (Mar. 30, 2020), https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html.

7. *Id.*

8. *Id.*

9. *Id.*

10. Kim A. Burger, Chief Bureau of Internet and Technology New York State Attorney General, Letter Agreement Between Zoom and the NYAG (May 7, 2020).

However, the same reports asserting that Zoom inappropriately shared user data with Facebook and then, later, other third-party entities, became the basis of the class action suit styled as *In Re: Zoom Video Communications, Inc. Privacy Litigation*, Case No. 5:20-CV-02155-LHK (N.D. Cal. San Jose Division July 7, 2020). The amended class action complaint alleges data mining from well-known online entities like LinkedIn and Facebook.[11] It also alleges violations of the Children's Online Privacy Protection Act, which were allegedly addressed in the Letter Agreement with the New York Attorney General's Office.[12] Additionally, it alleges seven causes of action against Zoom: invasion of privacy and violation of the California Constitution, Art. 1 § 1 (which also references the CCPA); negligence; breach of implied contract; breach of implied covenant of good faith and fair dealing; unjust enrichment; violation of Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 *et seq.*); violation of the California Consumer Legal Remedies Act (Cal. Civ. Code § 1750 *et seq.*); violation of Comprehensive Data Access and Fraud Act; and deceit by concealment (Cal. Civ. Code § 1710(3).[13] The ultimate result of this class action is still pending and will be watched.

B. *Other Updated Data Breach Notification Statutes*

As of this writing, all fifty states in the United States, the District of Columbia, Guam, Puerto Rico, and the United States Virgin Islands, have enacted legislation requiring data custodians to advise the residents of those jurisdictions when their personal data is the subject or potential subject of a data breach. During 2020, several jurisdictions updated and further modified their data breach notification statutes as set forth below.

1. Oregon

As of January 1, 2020, Oregon's data breach notification law, restyled as "Oregon Consumer Information Protection Act" (OCIPA) went into full force. Aside from the refreshing new acronym, the revision follows the general global trend in expanding the definition of *data breach* and *personal information* and adding definitions for *covered entity* and *vendor*.[14] The amendment also created several additional obligations.

OCIPA broadens the definition of "data breach" to include "unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains

11. In Re: Zoom Video Communications, Inc. Privacy Litigation, Case No. 5:20-CV-02155-LHK (N.D. Cal. San Jose Division), Consolidated Amended Class Action Compl. ¶¶ 93–98, 144.
12. *Id.* ¶¶ 152–157.
13. *See id.*
14. *See* Ore. Rev. Stat. § 646A.602.

or possesses."[15] Further, the definition now specifically includes user name or other information with which to access the consumer's account.[16] The statute contains a new definition for *covered entity* to mean any person that "owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occupation or volunteer activities," but specifically does not include vendors.[17] As a result, "covered entities" are obligated to send notices of such to consumers where a data breach occurs.[18]

While the provision for covered entities specifically excludes vendors, entities who contract with covered entities and only access or use the data on behalf of the covered entity, the statute was expanded to provide such entities with their own guidelines.[19] The statute places notification obligation upon vendors to notify the covered entities "as soon as practicable but no later than 10 days after the discovery of the breach in security or having a reason to believe that the breach of security occurred."[20] Similarly, the vendor must provide written notice of a breach to the Attorney General when more than 250 consumers are affected or where the number of consumers affected is not determinable.[21] Also continuing with the current trends, OCIPA specifies that those covered entities and vendors who are subject to and comply with HIPAA or the GBLA are entitled to assert compliance with those Acts as an affirmative defense.[22]

2. Texas

On January 1, 2020, amendments to the Texas Consumer Privacy Act, Tex. Bus. & Com. Code § 521.053, went into effect following the enactment of H.B. 4390. The Act now requires persons conducting business within the state of Texas to disclose a breach within sixty days of discovering the breach.[23] Additionally, the Act now mandates that the Attorney General must also be notified within sixty days after discovering the breach if it involves more than 250 Texas residents.[24] The bill also created the Texas Privacy Protection Advisory Council, which is "tasked with studying laws governing privacy and protection of information linked to a specific individual, technological device, or household and to make recommendations to the Legislature by September 1, 2020, concerning privacy and

15. *Id.* § 646A.602(1)(a) (emphasis added).
16. *See id.* § 646A.602(12)(a)(B).
17. *Id.* § 646A.602(5)(a), (b).
18. *See id.* § 646A.604.
19. *See id.* § 646A.602(19).
20. *Id.* § 646A.604(2)(a).
21. *See id.* § 646A.604(2)(c).
22. *See id.* § 646A.622.
23. *See* Tex. Bus. & Com. Code § 521.053(b).
24. *See id.* § 521.053(i).

protection of Texans' information."[25] The seventeen-page report produced by that Council provides a concise overview of Texas data privacy, other state laws, federal laws, and international laws as well as six proposals.[26] The report also recommends several additional areas of inquiry, from duties and responsibilities of third-party vendors, to Fourth Amendment protections.[27] At the time of writing, it is unclear whether the Texas legislature will take any steps included in the report.

3. Illinois

On January 1, 2020, an amendment to the Illinois Person Information Protection Act (PIPA) went into effect.[28] The amendment revamped the notification mandate so that an entity subject to the Act (defined as a "data collector") must notify the Illinois Attorney General where a single data breach affects more than 500 Illinois residents.[29] The data collector must provide, "in the most expedient time possible," a description of the breach, the number of residents affected, and any plans or steps taken, or to be taken, regarding the breach.[30] This information may ultimately be published by the Illinois Attorney General.[31] This notice provision largely comports with other mandatory notices to the state Attorney General's office, but does not require as much information as jurisdictions like Massachusetts and Washington.[32]

4. Washington

Since 2016, the state of Washington has continued to be a leader in data breach response by producing annual data breach reports. The reports summarize trends in data breaches and provide recommendations to the state legislature based on those trends. Based on the reports, effective March 1, 2020, Washington reduced the notification timeline to the Attorney General from forty-five days to thirty days, one of the shortest in the United States.[33] Further, the amendment broadened the definition of *personal information* to include one or more of the following: full date of birth; private authentication key to access a user record; identification numbers

25. Texas Privacy Protection Advisory Council Report (Sept. 2020), https://www.house.texas.gov/_media/pdf/committees/Texas-Privacy-Protection-Advisory-Council-Report.pdf.
26. *See id.*
27. *See id.*
28. *See* 815 Ill. Comp. Stat. § 530 *et seq*.
29. *See id.* § 530/10(e).
30. *See id.* § 530/10(e)(2).
31. *See id.*
32. *See* Mass. Gen. Laws ch. 93H, § 3; *see also* Wash. Rev. Code § 19.255.010(7).
33. *See* Wash. Rev. Code § 19.255.010–.020.

(student, military, or passport); any information about the consumer's medical history (mental or physical); and biometric information.[34] It also includes a consumer's username or email address in combination with another element that would permit access to a resident's online account.[35]

5. Vermont

Vermont's amended Security Breach Notice Act went into effect on July 1, 2020, along with the new Student Data Privacy law.[36] The amended breach notification statute provides an expanded definition for *personally identifiable information* (PII) to include, in combination with the individual's first name or initial, last name, and one or more of the following data points: a government-issued identification number (such as a tax, passport, or military identification number); biometric information; genetic information; and health information.[37] Importantly, the definition of a security breach was also amended to include those instances where an individual's login credentials (such as for an online account) are compromised.[38] A data breach consisting of login credentials triggers a fourteen-day notice requirement for the Vermont Attorney General's Office or Department of Financial Regulation under Title 8, but not where the login credentials are from the data breach of another entity and not the data collector or its agent.[39] The Act also modified the provisions permitting substituted service to include email service where the lowest cost would exceed $10,000, double the prior threshold of $5,000.[40] This substituted service is also permitted where the only information compromised is login credentials.[41] Data collectors are subject to the Vermont Data Breach Notification Act where the entity complies with HIPAA and HITECH.[42]

Vermont also enacted the Student Data Privacy law which generally prohibits certain online entities, referred to as "operators," from providing targeted advertising derived from information gleaned through the use of the operator's site or application, when that application or site is used for an educational purpose in conjunction with a preK–12 school.[43]

34. *See id.* § 19.255.005.
35. *See id.*
36. *See* Vt. Stat. Ann. tit. 9, §§ 2430, 2435.
37. *See id.* § 2430(10)(A).
38. *See id.* § 2435(b).
39. *See id.* §§ 2435(b)(1), (3)(D).
40. *See id.* § 2435(b)(6)(B).
41. *See id.* § 2435(d)(3).
42. *See id.* § 2435(e).
43. *See id.* § 2443(a).

6. Virginia

As of July 1, 2020, the definition of personal information included the first initial and last name in combination with, or otherwise linked to, a resident's passport number or military identification number.[44] Virginia, much like Vermont, requires notice to the consumer and the Attorney General's office whenever the personal information of *any* resident of the Commonwealth is "acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud. . . ."[45]

7. Washington, D.C.

As of May 19, 2020, D.C. also has a broader definition of personal information to include many of the same data points as the newly revamped Washington and Vermont laws. Specifically, the definition now includes government-issued identification numbers (including taxpayer, passport, or military identification numbers); account number (such as a credit card that would permit access to the consumer's financial accounts); medical information; genetic information and DNA profile; health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer that permits access to an individual's health and billing information; biometric data; and any combination of data elements listed above, that would enable a person to commit identity theft without reference to the individual's name.[46]

The definition also includes a resident's "user name or e-mail address in combination with a password, security question and answer, or other means of authentication, or any combination of data elements . . . [from the above list] that permits access to an individual's e-mail account."[47] The amendment broadens the amount of information required in the consumer notices to include information about the personal information lost, a free security freeze, a right to certain identity theft services for a period of eighteen months, and contact information for the appropriate reporting entity, such as the Attorney General's office.[48] Where the subject breach involves more than fifty D.C. residents, a notice must be filed with the Attorney General's office with a description of the breach, the information compromised, and the remedial action.[49] Conforming with many other data breach notification laws, the amendment provided a partial exemption for those entities which are subject to and comply with the breach notification rules

44. *See* Va. Code Ann. § 18.2(A).
45. *See id.* § 18.2(B).
46. D.C. Code § 28-3851(3)(A)(i).
47. *Id.* § 28-3851(3)(A)(ii).
48. *See id.* § 28-3852(A)(a-1); *see also id.* §28-3852b.
49. *See id.* § 28-3852(B)(b-1).

contained in the GLBA, HIPAA, and HITECH, but still requires notice to be provided to the Attorney General's office.[50] Lastly, the amendment modifies the damages section of the statute and deems a violation of the chapter to be an unfair or deceptive trade practice.[51]

II. CASE LAW DEVELOPMENTS

A. *Insurance Coverage Cases*

The area of cyber coverage is rapidly evolving. However, like a shadow, "silent cyber" coverage lurks. While there are policies designed to cover such events as ransomware attacks and data breaches expressly, courts will sometimes find the same coverage in a Commercial General Liability policy, Business Owner's Policy, or Director's and Officer's policies. Because insurance is the predominate method of managing risk, we include a summary of the most recent developments in the insurance market to help guide the assessment and management of emerging risks. The highlights are set forth below.

1. Silent Cyber Coverage

A Brief Background. Silent cyber refers to potential cyber-related losses stemming from traditional property and liability policies that were not specifically designed to cover cyber risk. "Silent cyber," also known as "unintended" or "non-affirmative" cyber, refers to the unknown or unquantified exposures originating from cyber perils that may trigger traditional property and liability insurance policies.[52] Silent cyber situations can arise in different insurance coverage areas. In fact, issues can arise wherever technology is present. Traditional liability or property policies were not designed with cyber exposures in mind and, therefore, do not expressly include coverage for cyber risks.[53] The coverage risk to an insured with a traditional property or other casualty liability policy can result in a silent cyber scenario. With people online now more than ever, many companies have elected to procure policies to protect their vulnerable data as people work remotely. Many companies still operate under the belief that a general liability policy will cover this risk and that they do not need a standalone cyber policy.

50. *See id.* § 28-3852(B)(b-2); *see also id.* § 28-3852a(d).

51. *See id.* § 28-3852c(b).

52. Guy Carpenter, *Affirmative vs. Silent Cyber: An Overview*, Marsh & McLennan Cos. (Oct. 2018), http://www.guycarp.com/content/dam/guycarp/en/documents/library/2019/Affirmative%20vs.%20Silent%20Cyber%20An%20Overview.pdf.

53. *The Problem of Silent Cyber Risk Accumulation*, Willis Towers Watson (Feb. 25, 2020), https://www.willistowerswatson.com/en-US/Insights/2020/02/the-problem-of-silent-cyber-risk-accumulation.

Mark Synott of Willis Towers Watson, posited "under property forms, does data constitute 'property' and does an unattributed malware attack trigger the War Exclusion?"[54] As illustrative of this conundrum, Synott proffers one of the most well-known cyber-attacks in history, the 2017 NotPetya attack.[55] The NotPetya attack ravaged a range of businesses from shipping ports and supermarkets to ad agencies and law firms, by encrypting their master files and demanding a Bitcoin ransom to restore access to those files.[56] Most victims were based in Ukraine, but several global corporations were also infected, including shipping giant Maersk, "responsible for 76 ports on all sides of the earth and nearly 800 seafaring vessels, including container ships carrying tens of millions of tons of cargo, representing close to a fifth of the entire world's shipping capacity, was dead in the water."[57] The losses stemming from the NotPetya attack "resulted in silent cyber losses on non-cyber lines of business for various insurers."[58] So, while "silent cyber" was a known risk in the insurance circle, the NotPetya attack and its immediate predecessor, WannaCry, appeared to inspire global insurers to start to address the issue of liability.[59]

Attempts to remediate silent cyber: Starting in 2019, the insurer Allianz advised that its Global Corporate and Specialty unit would update "coverage in 2019 to provide clarity so that physical damage and bodily injury arising from cyber events would generally continue to be covered under corporate, commercial and specialty policies whereas cyber-related 'pure financial loss' without physical damage or injury would be covered under specific cyber policies only."[60] Caroline Dunn, Head of Class of Business, Performance Management, at Lloyd's of London, stated the following in a July 4, 2019, *Market Bulletin* to provide clarity for Lloyd's customers for cyber exposures:

> Lloyd's view is that it is in the best interests of customers, brokers and syndicates for all policies to be clear on whether coverage is provided for losses caused by a cyber event. This clarity should be provided either by excluding coverage or by providing affirmative coverage in the (re)insurance policy. For the avoidance of doubt, Lloyd's view policies where no exclusion exists and there is no express grant of cyber coverage as 'non-affirmative'. In all these

54. *Id.*
55. *See id.*
56. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired.com (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.
57. *Id.*
58. Bethan Moorcraft, *What Is Silent Cyber Risk?*, Ins. Bus. Am. (Nov. 26, 2018), https://www.insurancebusinessmag.com/us/guides/what-is-silent-cyber-risk-117150.aspx.
59. *The Problem of Silent Cyber Risk Accumulation*, *supra* note 53.
60. *Id.*

> cases action should be taken to provide clarity of coverage for customers to comply with this requirement.[61]

According to a subsequent *Lloyd's Bulletin*, issued on January 28, 2020, the underwriters were required to use "clear language to affirm or exclude cyber cover for all [first-party property] policies incepting on or after 1 January 2020."[62] Indeed, according to the proffered four-phase timeline, all Lloyd's polices will contain clear language regarding cyber coverage by July 1, 2021.[63] The success of these policies and efforts remains to be seen and will continue to be tested against prior insurance policies, as claims may arise from offsite work on personal devices where the COVID-19 pandemic has forced people to work from home.

2. *National Ink and Stitch, LLC v. State Auto Property & Casualty Insurance Co.*

A pre-pandemic case that illustrates these concerns comes from the District Court for the District of Maryland's decision in *National Ink and Stitch, LLC, v. State Auto Property and Casualty Insurance Company*, which addressed the silent cyber scenario when addressing a policy's interpretation of data loss versus property loss.[64]

Plaintiff, National Ink & Stitch, LLC (National Ink), asserted an action against State Auto Property and Casualty Insurance Company (State Auto), its businessowner's insurance carrier, seeking coverage for damage alleged to have been sustained to its computer system in a ransomware attack.[65] National Ink obtained the policy to cover its embroidery and screen printing business.[66] National Ink stored most, if not all, facets of its business on the servers for both the creative and administrative aspects (e.g., art, logos, designs for its business, graphic arts software, shop management software, embroidery software, and webstore management software).[67]

The facts of the matter are simple. In December 2016, a ransomware attack rendered the server virtually inaccessible and unusable, except for the embroidery software.[68] After producing the ransomware payment, the

---

61. Caroline Dunn, *Providing Clarity for Lloyd's Customers on Coverage for Cyber Exposures*, Lloyd's of London Market Bull. (July 4, 2019), https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2019/07/y5258.pdf.

62. Caroline Dunn, *Update—Providing Clarity for Lloyd's Customers on Coverage for Cyber Exposures*, Lloyd's of London Market Bull. (Jan. 29, 2020), https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2020/1/y5277-update--providing-clarity-for-lloyds-customers-on-coverage-for-cyber-exposures.pdf.

63. *See id.*

64. *See* Nat'l Ink & Stitch, LLC v. State Auto. Prop. & Cas. Ins. Co., 435 F. Supp. 3d 679, 680 (D. Md. 2020).

65. *See id.*

66. *See id.*

67. *See id.*

68. *See id.*

server was restored.[69] However, even after a computer security company cleared the server and reinstalled the software and protective software, the system was noticeably slower and less efficient, and it likely concealed remnants of the ransomware virus.[70] Additionally, all the designs stored on the server, the data, were lost.[71] National Ink sought replacement costs for its hardware and software—in other words, its entire computer system.[72]

State Auto denied the claim to reimburse National Ink for a new computer system, finding that the ransomware attack did not constitute a physical loss eligible for reimbursement from the policy, as the loss was "only lost data, an intangible asset, and National Ink could still use its computer system to operate its business."[73] The court disagreed and found that National Ink could seek reimbursement under either "(1) the loss of data and software in its computer system, or (2) the loss of functionality to the computer system itself."[74]

"Maryland follows the law of objective contract interpretation"[75] and "the written language embodying the terms of an agreement will govern the rights and liabilities of the parties, irrespective of the intent of the parties at the time they entered the contract."[76] The court found that because the policy included items such as "software" and "data" as a definition for "Electronic Media" as "Covered Property," the policy covered National Ink's lost software and data and was not limited to only tangible property.[77] Similarly, the court determined that the terms of the policy did not limit coverage to only those instances where the computer was rendered entirely unusable.[78] Rather, it found that because the definition was compensation for "direct physical loss *or damage*," the lost or decreased functionality would be covered.[79]

The effects of the COVID-19 Pandemic and anticipated increase of silent cyber risks. According to Willis Towers Watson's Report, fifty-seven percent of respondents believe that the COVID-19 pandemic has increased

69. *See id.*
70. *See id.* at 680–81.
71. *See id.*
72. *See id.*
73. *Id.* at 682. The policy provided that "State Auto . . . will pay for direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from any Covered Cause of Loss." And the "Computer Coverage endorsement expressly defines 'Covered Property' to include 'Electronic Media and Records (Including Software),' and defines 'Electronic Media and Records' to include: (a) Electronic data processing, recording or storage media such as films, tapes, discs, drums or cells; (b) Data stored on such media. . . ." *Id.* at 681.
74. *Id.* at 682.
75. Sy-Lene of Wash., Inc. v. Starwood Urb. Retail II, LLC, 829 A.2d 540 (Md. 2003).
76. Long v. State, 807 A.2d 1 (Md. 2002).
77. *Nat'l Ink & Stitch, LLC*, 435 F. Supp. 3d at 683–84.
78. *See id.* at 685–86.
79. *See id.* (emphasis added).

silent cyber risks.[80] As stated above, Lloyd's approach is to redress this global problem in the property and casualty market internally: insurers are exposed to silent cyber risks because the presentation of such claims under traditional policies may result in the affirmation of coverage if the policy language is not explicit as to cyber events. Others believe that silent cyber risks can be mitigated by taking such steps as "[i]dentifying classes of business and policy types that are particularly vulnerable to residual silent cyber loss leakage . . . [and] [d]eveloping approaches to pricing and capital setting for silent cyber risk."[81] Jeremy Barnett of Tokio Marine, HCC, stated in October 2019, "We have seen a 6x increase in ransomware attacks over the last four years, and that's mostly small business, and the costs of responding to those ransomware attacks are up almost tenfold over the last two years."[82] While these are the first small steps in managing silent cyber risk, it is reasonable to expect that the leaps to come will be commensurate with the as yet unidentified risks until insurance coverage more firmly focused on cybersecurity and data privacy takes hold.

B. *Biometric Privacy*

The last survey period has been a busy one for the topic of the Illinois Biometric Information Privacy Act (Illinois BIPA).[83] While several other states have biometric privacy acts in place, the Illinois law is the only one that permits a private right of action. Two cases in particular are of note.

1. Federal Jurisdiction

In *Bryant v. Compass Group U.S.A., Inc.*,[84] plaintiff Christine Bryant provided her fingerprint data to Compass Group USA to use the vending machines in the office. Section 15(b) of the Illinois BIPA provides that a person, including employees and customers, must knowingly provide consent for any party to collect and use biometric identifiers and information.[85] The Seventh Circuit held that the plaintiff's informed consent claim alleged more than a mere procedural violation against the defendant, who allegedly collected and distributed plaintiff's biometric information in violation of Section 15(b). The Seventh Circuit explained that depriving a plaintiff's ability to choose whether or not to consent to this use of her biometric information constituted a "concrete and particularized injury-in-fact" that

80. *COVID-19 Has Changed How We Think About Cyber Risk*, Willis Towers Watson (Sept. 23, 2020), https://www.willistowerswatson.com/en-US/Insights/2020/09/covid-19-has-changed-how-we-think-about-cyber-risk.

81. Guy Carpenter, *Silent Cyber No Longer Silent? Part One*, MarshMcLennan (July 22, 2020), https://www.gccapitalideas.com/2020/07/22/silent-cyber-no-longer-silent.

82. *The Problem of Silent Cyber Risk Accumulation*, *supra* note 53.

83. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14.

84. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).

85. 740 Ill. Comp. Stat. 14/15(b).

was sufficient to confer Article III standing for the Section 15(b) claim.[86] The Seventh Circuit held that the plaintiff did not have Article III standing to pursue her claim under Section 15(a),[87] which requires a private entity to develop a written policy concerning the retention and destruction of biometric data and identifiers. In a clarification opinion issued in June 2020,[88] the Seventh Circuit clarified that 15(a) claims are separate from 15(b) claims and that its opinion was limited to 15(a), as plaintiff alleged a claim under part of 15(a), which requires the "development of a written policy, made available to the public," rather than a claim under a subsequent part of 15(a), "requiring compliance with the established retention schedule and destruction guidelines."[89] For now, the case clarifies what kinds of injuries supply Article III standing for Illinois BIPA claims brought in federal court.

2. Workers' Compensation Issues

In a second case of importance with respect to the Illinois BIPA, an Illinois appellate court investigated the issue of whether Workers' Compensation was the sole remedy for an employee who alleged violations of the Illinois BIPA. In *McDonald v Symphony Bronzeville Park LLC*,[90] the court held that the exclusive remedy of Workers' Compensation does not prohibit employees from bringing an action against an employer for allegedly violating the Illinois BIPA. While acknowledging that the Illinois Supreme Court "has indicated that the [Compensation Act] generally provides the exclusive means by which an employee can recover against an employer for a work-related injury,"[91] the court found that the exception for "not compensable" under the Workers' Compensation Act provided the out for the plaintiff in this case, holding:

> In light of the above discussion, we fail to see how a claim by an employee against an employer for liquidated damages under the Privacy Act—available without any further compensable actual damages being alleged or sustained and designed in part to have a preventative and deterrent effect—represents the type of injury that categorically fits within the purview of the Compensation Act, which is a remedial statute designed to provide financial protection for workers that have sustained an actual injury. As such, we conclude that the exclusivity provisions of the Compensation Act do not bar a claim for

86. *Bryant*, 958 F.3d at 620–21.
87. 740 Ill. Comp. Stat. 14/15(a).
88. Bryant v. Compass Grp. USA, Inc., 2020 WL 6534581 (7th Cir. June 30, 2020).
89. *Id.* at *1.
90. McDonald v Symphony Bronzeville Park LLC, No. 1-19-2398, 2020 WL 5592607, ¶ 14 (Sept. 18, 2020).
91. *Id.* ¶ 18.

statutory, liquidated damages, where an employer is alleged to have violated an employee's statutory privacy rights under the Privacy Act, as such a claim is simply not compensable under the Compensation Act.[92]

3. Conclusion

The Illinois BIPA in recent years has increasingly been the subject of review by the federal and state courts and will continue to be a hot topic in the coming years.

C. *Right to Privacy*

The debate over digital privacy is constantly evolving in the United States. One area that shows this evolution is the employment field, especially when related to criminal proceedings. The evolving intricacies and nuances of digital privacy law can pose a pitfall to the unwary, even over seemingly minor details.

1. *Walker v. Coffey*, No. 19-1067 (3d Cir. 2020).

In *Walker v. Coffey*, the Third Circuit dismissed the plaintiff's claims that the defendants violated 18 U.S.C. Chapter 121, §§ 2701–2712, collectively known as the Stored Communications Act (SCA).[93] The plaintiff had argued that the defendants—two government employees from the Pennsylvania Office of the Attorney General (OAG) that had been conducting a criminal investigation relating to the plaintiff's husband and his company—had "violated provisions of the" SCA "by inducing her employer, Pennsylvania State University (Penn State), to disclose her work emails with a facially invalid subpoena."[94]

Penn State had refused to produce plaintiff's work emails to the defendants without a subpoena.[95] The defendants subsequently presented a subpoena to Penn State; however, as later conceded by the OAG, the "subpoena was incomplete and therefore unenforceable."[96] In response to the subpoena, "Penn State's Assistant General Counsel 'instructed an employee in her office to assist with the production of [her] emails,' choosing to cooperate 'rather than contest the validity of the subpoena or otherwise limit any search.'"[97] A panel of the Third Circuit had previously

92. *Id.* ¶ 27.
93. Walker v. Coffey, 956 F.3d 163, 171 (3d Cir. 2020).
94. *Id.* at 164.
95. *Id.*
96. *Id.* at 165. A panel of the Third Circuit also ruled previously that the subpoena was facially invalid. Walker v. Coffey, 905 F.3d 138, 150 (3d Cir. 2018).
97. *Coffey*, 956 F.3d at 170 (quoting *Coffey*, 905 F.3d at 149–50).

ruled that this action amounted to a voluntary disclosure,[98] rather than one "under coercion resulting from the invalid subpoena,"[99] and as a result was "law of the case."[100] Despite acknowledging that voluntarily disclosing the emails "independent[] of the illegal subpoena [wa]s fatal to her claim," the plaintiff made no attempt to even allege that the disclosure was the result of receipt of the subpoena.[101]

2. *United States v. Moore-Bush*, 963 F.3d 29 (1st Cir. 2020) and *United States v. Yang*, 958 F.3d 851 (9th Cir. 2020)

In 2020, two cases—one from either coast—tested the limits of the right to privacy under the Fourth Amendment as set forth in 2018 by the Supreme Court in *Carpenter v. United States*.[102] *Carpenter* involved the continued monitoring of an individual's movements through cellphone tracking.[103] *United States v. Moore-Bush* involves installing an unwarranted pole camera outside the defendant's home to take constant silent video.[104] The pole camera remained in place for approximately eight months. It was fixed

98. *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1074–75 (9th Cir. 2004) ("Fighting a subpoena in court is not cheap, and many may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake. Because defendants procured consent by exploiting a mistake of which they had constructive knowledge, the district court erred by dismissing based on that consent."); Crow v. Uintah Basin Elec. Telecomm., No. 2:09–CV–1010, 2010 WL 5069852, at *3–4 (D. Utah Dec. 6, 2010) (finding that plaintiff stated SCA claim by pleading that defendant obtained consent of communication service provider to access text messages through fraud); Pietrylo v. Hillstone Rest. Grp., No. 06–5754, 2008 WL 6085437, at *4 (D.N.J. July 25, 2008) (denying summary judgment to employer where employee alleged that she provided private social networking site password to employer under fear of adverse employment action, noting that, "[i]f her consent was only given under duress, then the [d]efendants were not 'authorized' under the [SCA]").

99. *Coffey*, 956 F.3d at 165.

100. *Id.* at 170 (quoting *In re* City of Phila. Litig., 158 F.3d 711, 717 (3d Cir. 1998)) ("The law of the case doctrine dictates that 'one panel of an appellate court generally will not reconsider questions that another panel has decided on a prior appeal in the same case.'").

101. *Id.*; *see also* Garcia v. Haskett, No. C 05–3754 CW, 2006 WL 1821232, at *5 (N.D. Cal. June 30, 2006) (holding that, although defendant may have illegally accessed the facility of third-party non-defendant ISP by accessing plaintiff's e-mail account, plaintiff nonetheless failed to state SCA claim because she did not allege that defendant's access of her stored e-mails "was conduct unauthorized by" the ISP); Oce N. Am., Inc. v. MCS Servs., Inc., 748 F. Supp. 2d 481, 487 (D. Md. 2010) (noting that plaintiff failed to state claim under Computer Fraud and Abuse Act (CFAA) where no allegation that "person with the requisite authority . . . denied access such that [d]efendants' access was unauthorized or in excess of its authorization").

102. Carpenter v. United States, 138 S. Ct. 2206 (2018).

103. *See id.* at 2217 (2018) ("[With] the ability to chronicle a person's past movements through the record of his cell phone signals . . . we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through . . . [a cell phone tracking device].").

104. United States v. Moore-Bush, 963 F.3d 29, 33 (1st Cir. 2020).

outside the home and could not record any sound or any information that was inside the house or beyond the capability of an average passerby.[105] The First Circuit found that "[p]ole cameras are a conventional surveillance technique and are easily thought to be a species of surveillance security cameras."[106] As such, pole cameras "are conventional, not new, technology [and] are the exact kind of conventional surveillance technique" permitted in *Carpenter*.[107] Further, the First Circuit found that while the "unrelenting" surveillance existed, it did not infringe a privacy right, as "[a]ny home located on a busy public street is subject to the unrelenting gaze of passersby, yet '[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.'"[108]

In *United States v. Yang*, the issue was whether a right to privacy prohibited photographing and tracking a vehicle with an Automatic License Plate Recognition (ALPR) technology.[109] The defendant was "observed on surveillance cameras driving a rented GMC Yukon and stealing mail out of collection boxes" in Las Vegas, Nevada.[110] The Yukon was rented from a third-party company, and the rental company had attempted to repossess the Yukon as it was several days overdue.[111] The Postal Inspector used ALPR to search a database of license plate photos captured by camera-mounted vehicles to try and track the defendant down using his historical location data.[112] The Ninth Circuit concluded that "Yang has failed to establish that he has a reasonable expectation of privacy in the historical location information of the Yukon, . . . [and t]here is no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle."[113] Of note, the majority opinion does not address whether such historical tracking through a near real-time license plate database would be an invasion of the right to privacy or if it would violate a right to privacy if the database was the target of a hack and bad actors had used it. Rather, the

105. *See id.* 33–35.
106. *Id.* at 31.
107. *Id.* at 40 (internal citations omitted).
108. *Id.* at 42 (quoting California v. Ciraolo, 476 U.S. 207, 213, (1986)).
109. United States v. Yang, 958 F.3d 851, 853 (9th Cir. 2020).
110. *Id.* at 852.
111. *See id.*
112. *See id.*
113. *Id. at* 859 ("In so holding, we find instructive our decisions in *United States v. Dorais*, 241 F.3d 1124, 1129 (9th Cir. 2001) and *United States v. Henderson*, 241 F.3d 638 (9th Cir. 2000) which both analyze a lessee's expectation of privacy in rental property after the expiration of the rental period.").

court relied on the breach of the contractual relationship between the lessor and lessee to determine the right to privacy and avoid the broader issue.

Carpenter can be read to permit certain collection activities that could amount to such a pervasive intrusion as to violate the reasonable expectation of privacy, but courts appear to be resistant to addressing this issue. Both *Moore-Bush* and *Yang* explore this issue solely in the criminal context; it would be interesting to see how the right to privacy fares when these law enforcement practices are subjected to a breach from a hacker.