LEGAL ISSUES AND A CHECKLIST FOR RESPONDING TO RANSOMWARE ATTACKS

Excerpted from the forthcoming 2023 update to Chapter 27
(Cybersecurity: Information, Network and Data Security)
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

INTERNET AND MOBILE LAW AND LITIGATION TRENDS

INTUIT

MARCH 8, 2023

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:	Los Angeles:	Washington, D.C.:
1900 University Avenue, 5th Fl.	1840 Century Park East, Ste. 1900	2101 L Street, N.W., Ste. 1000
East Palo Alto, CA 914303	Los Angeles, CA 90067	Washington, D.C. 20037
Direct Dial: (650) 289-7881	Direct Dial: (310) 586-6575	Direct Dial: (202) 331-3138
Direct Fax: (650) 462-7881	Direct Fax: (310) 586-0575	Fax: (202) 331-3101

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West 2023 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net

GT GreenbergTraurig

Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal Circuits
U.S. Supreme Court
JD, LLM, CIPP/US

Ballon@gtlaw.com
LinkedIn, Twitter, Facebook: IanBallon

Silicon Valley
1900 University Avenue
5th Floor
East Palo Alto, CA 94303
T 650.289.7881
F 650.462.7881

Los Angeles
1840 Century Park East
Suite 1900
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Washington, D.C.
2101 L Street, N.W.
Suite 1000
Washington, DC 20037
T 202.331.3138
F 202.331.3101

Ian C. Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and AdTech class action suits.

Ian has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2022). He has been listed in Best Lawyers in America consistently every year since 2003 and was named Lawyer of the Year for Information Technology in 2023, 2022, 2020, 2019, 2018, 2016 and 2013. In 2022, 2021, 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and he has been included on the *Daily Journal's* annual list of the Top 100 Lawyers in California. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal and he has been* recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's Vanguard Award for significant contributions to the development of intellectual property law. Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named a Northern California Super Lawyer every year from 2004 through 2021 and a Southern California Super Lawyer for every year from 2007-2021. He has also been listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian is also the author of the leading treatise on internet and mobile law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). In addition, he serves as Executive Director of Stanford University Law School's Center for the Digital Economy. He also chairs PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian holds JD and LLM degrees and the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 3

THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

ault/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

- COSO, *Risk Assessment in Practice*, https://www.coso.org/Documents/COSO-ERM%20Risk%20Assessment%20in%20Practice%20Thought%20Paper%20October%202012.pdf

2. Developing a Comprehensive Written Information Security Program

- NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 16, 2018); https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Updated Aug. 2017), https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
- ISO/IEC 27001:2013 (Information technology—Security techniques—Information security management systems—Requirements), https://www.iso.org/isoiec-27001-information-security.html
- Mass. Office of Consumer Affairs and Business Regulation, *A Small Business Guide: Formulating a Comprehensive Written Information Security Program*, https://archives.lib.state.ma.us/bitstream/handle/2452/685875/ocn987380700.pdf?sequence=1&isAllowed=y
- Peter Sloan, *The Reasonable Information Security Program*, 21 Rich. J.L. & Tech. 2 (Nov. 21, 2014)

3. Examples of a WISP

- Example of NIST 800-53 Template—http://examples.complianceforge.com/example-nist-800-53-written-information-security-program-it-security-policy-example.pdf
- Wellesley College—http://www.wellesley.edu/lts/policies/wisp
- Buchanan & Associates—Sample template—https://www.buchananassociates.com/Buchanan-Associates-Sample-Template-Written-Information-Security-Plan-WISP.pdf
- New England Teamsters Pension Fund—http://nettipf.com/pdf_files/wisp.pdf

27.14 Legal Issues and A Checklist for Responding to Ransomware Attacks

A ransomware attack involves a security breach where an

unauthorized third party gains access to a network and encrypts data or systems, to prevent the owner from using its essential systems or data until a "ransom" is paid (typically in cryptocurrency[1]) for a decryption key, often accompanied by the threat that sensitive data stolen from the target company will be released if the ransom is not paid. Unlike a typical cybersecurity breach where a third party gains access to a network and copies information that it seeks to use itself or monetize, a ransomware attack is undertaken to obtain money—a ransom[2]—from the target of

---

[Section 27.14]

[1]The increasing frequency in ransomware attacks during the 2010s tracked the rise in acceptance of cryptocurrency, which generally allows for anonymous transactions. In 2021, however, the FBI was able to track disbursement of approximately $4.4 million in cryptocurrency paid to DarkSide as a ransom for the Colonial Pipeline Co. ransomware attack, and recover cryptocurrency worth approximately $2.3 million. *See* David Uberti, *How the FBI Got Colonial Pipeline's Ransom Money Back,* Wall St. J., June 11, 2021. Cryptocurrencies are held in digital accounts known as wallets, which store the addresses for the virtual locations of cryptocurrency and the private keys needed to access the funds. While wallets are generally private, cryptocurrency transactions are recorded on the Blockchain, a public ledger that is visible to third parties, including law enforcement. *See id.*; *see also supra* § 27.03A (blockchain).

While cryptocurrency exchanges generally are used for lawful purposes, SUEX OTC, S.R.O. was placed on the OFAC sanctions list in September 2021, based on a finding that more than 40% of its known transactions involved illicit actors and that SUEX had facilitated transactions involving at least eight ransomware variants. *See* U.S. Department of the Treasury, *Treasury Takes Robust Actions to Counter Ransomware,* Sept. 21, 2021.

[2]Ransom demands may vary depending on the size of an enterprise, its ability to pay, and the extent of its insurance coverage. REvil, a Russian ransomware attacker identified by the FBI, reportedly obtained an $11 million payment for a Memorial Day 2021 attack on global meat supplier JBS and demanded $70 million in cryptocurrency for a universal decryptor in response to the attack on Kaseya, a software company that provided remote IT services to up to over 800,000 businesses located around the world, which was discovered at the beginning of the July 4 holiday weekend in 2021. *See* Ben Kochman, *Software Vendor Hack Leads to Ransomware Spree,* Law360, July 6, 2021.

While it is difficult to accurately estimate the average ransomware payment since information on payments is incomplete and payment amounts often depend on individual negotiations and various factors such as the extent of insurance coverage and a company's need to obtain a decryption tool, Coveware estimated that ransomware payments declined in 2021 as a result of ransomware being treated as a national security concern, fewer companies making ransom payments, and ransomware at-

the attack (usually in the form of anonymized cryptocurrency), in return for a decryption key to allow the target to regain access to systems or data that had been rendered inaccessible and/or to prevent its public disclosure. A ransomware attacker typically will disclose some data to the victim to prove to the owner that the person or organization making the ransom demand is the same person or organization that encrypted it (since otherwise a company could be doubly victimized by paying the wrong scammer). Target companies typically must react quickly—especially if their ability to conduct business is implicated. Adding to the complexity of responding to a ransomware attack, however, is the fact that paying or even simply facilitating ransomware payments to persons, entities or countries subject to U.S. sanctions or embargoes, may subject a person to civil penalties and fines imposed the U.S. Treasury Department's Office of Foreign Asset Controls (OFAC).

OFAC sanctions may be imposed on businesses that directly pay or facilitate ransomware payments to on behalf of victims, including, according to OFAC, financial institutions, cyber insurance providers, forensic firms and others,[3] based on strict liability. Pursuant to the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[4] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (such as Cuba, Russian occupied Crimea, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, includ-

---

tackers targeting smaller companies that were less well prepared to withstand an attack. *See* Coveware Ransomware Recovery Blog, https://www.coveware.com/blog (last visited Dec. 26, 2021).

The costs associated with remediating a ransomware attack are not limited to the ransom payment, if any. Whether addressed exclusively through backups or with a decryptor purchased for a ransom, a target company will need to expend significant time and money to restore and harden the security of its software, networks and data following a ransomware attack.

[3] *See* U.S. Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,* Sept. 21, 2021, *available at* https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[4] 50 U.S.C.A. §§ 4301–41, 1701–06.

ing a transaction by a non-U.S. person that causes a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations.[5] For this reason, businesses need to act cautiously in evaluating whether to accede to ransom demands.

As ransomware attacks have become more prevalent, accounting for 22% of cyberattacks in 2021 by one estimate,[6] some criminal enterprises have reduced ransomware attacks to an organized business, typically run offshore (in Russia and elsewhere), with predictable demands and sought-after terms for resolving an attack.[7] Lawyers who deal regularly with ransomware attacks will recognize particular criminal

---

[5]U.S. Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,* Sept. 21, 2021, *available at* https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf; *see also* 31 C.F.R. part 501, appx. A (OFAC's Economic Sanctions Enforcement Guidelines). Although knowledge or intent are not determining factors (since OFAC sanctions may be imposed based on strict liability), OFAC will consider the existence, nature and adequacy of a sanctions compliance program in determining an appropriate enforcement response to an apparent violation. *See Updated Advisory,* at 4; *see also* Cybersecurity and Infrastructure Security Agency Guidance, *Ransomware Guide,* Sept. 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf. Mitigating factors "could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others." *Updated Advisory,* at 5. "While the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took the mitigating steps described above, particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation." *Id.*

[6]Bree Fowler, *Data breaches break record in 2021*, c/net, Jan 24, 2022 (quoting the Identity Theft Resource Center's 2021 Data Breach Report).

[7]Some have dubbed this more organized approach of groups such as REvil and DarkSide as *ransomware-as-a-service,* suggesting that like cloud-based SaaS application providers, they offer tools and services used by others. *See* Gerrit De Vynck, Rachel Lerman, Ellen Nakashima & Chris Alcantara, *The anatomy of a ransomware attack,* Wash. Post, July 9, 2021; Isabelle Khurshudyan & Loveday Morris, *Ransomware's suspected Russian roots point to a long détente between the Kremlin and hackers,* Wash.

organizations, which have set practices, follow particular routines, and are known to make particular demands or be willing to negotiate particular settlement terms. At the same time, efforts by the Biden Administration to pressure Russia to shutter ransomware groups based in Russia, beginning in 2021, have reduced somewhat the volume of attacks.[8]

When a ransomware attack occurs, the victim company typically must confront two separate but related concerns: (1) access to critical systems or information, which have become inaccessible, and (2) the compromise of information that has been exfiltrated, which could be further disseminated or publicly disclosed.

Following a ransomware attack, there is often pressure on the target of the attack to act quickly. If a business does not have adequate backup copies of its data or the ability to operate without accessing a compromised system, the business could be shut down for days or even weeks until it regains access to its data, systems or network. A business also may be under pressure to inform customers and vendors if data or systems are inaccessible, and may face regulatory pressure to quickly report a breach if data has been exfiltrated. The ransom demand itself typically establishes a deadline for a response.

Ransomware attackers may also feel pressure to close a transaction quickly before they are unmasked, which may allow room for negotiating the amount of the ransom payment.

Ransomware attackers typically offer the ability to regain access coupled with the threat to release sensitive informa-

---

Post, June 12, 2021; *see also* Andrew E. Kramer, Michael Schwirtz & Anton Troianovski, *Secret Chats Show How Cybergang Became a Ransomware Powerhouse,* N.Y. Times, June 3, 2021 (describing how DarkSide, as the malware developer, charged a user fee to affiliates, who used DarkSide software to break into victim networks, and even provided technical support for hackers, negotiating with targets, processing payments, and developing pressure campaigns, with DarkSide earning fees on a sliding scale ranging from 25% for ransoms under $500,000 to 10% for ransoms over $5 million).

[8]Shortly after President Biden demanded that Russian President Putin crack down on ransomware attackers based in Russia that targeted American entities, REvil's darknet (.onion) and clearnet (decoder.re) websites went dark. David E. Sanger, *Russia's most aggressive ransomware group disappeared,* N.Y. Times, July 13, 2021; Maggie Miller, *Russian hacking group believed to be behind Kaseya cyber attack goes offline,* The Hill, July 13, 2021.

tion to the public if a ransom is not paid. When deals are made, ransomware attackers typically promise to honor their agreements and not further use, disseminate or retain the company's data or information once a ransom is paid. These commitments may be honored by attackers who are concerned about their reputations—and their ability to extract ransoms from other victims—but ransomware attackers ultimately are criminals, whose credibility and trustworthiness may be questionable.

Network and data access may be restored without paying a ransom if the company has adequate back up files and redundant capacity. If a company is unable to access its system or critical information, its business may be interrupted and it may face financial consequences that may a ransom payment appear reasonable. Even if a ransom is paid, there is no guaranty that a business can quickly resume operations. Some attackers are more skilled than others, and the process of encrypting and then decrypting files may not be bug-free. Decryption tools may be only as sophisticated as the criminals who created them. In many cases, it may be easier to prevent an owner from accessing critical systems or information than it is to restore them to working conditions. In addition, ransomware attackers have a greater incentive to engineer a detection-free attack than to create best-in-breed decryption and restoration tools. Victims that pay a ransom for decryption tools also must be careful to determine whether an attacker has created backdoors that would allow for future attacks or otherwise intentionally or unintentionally inserted malware or security flaws into a system.

With respect to data, although a victim typically may be deprived of access to information it needs to run its business, it may also face competitive, privacy or regulatory risks as a result of the exposure and possible further dissemination or publication of its information. The threat of publicizing company, employee or consumer information may not present as immediate a threat as being locked out of a system or network but the long term consequences for a company could be more significant.[9] Businesses that reject ransom demands may also face further extortion efforts,

[9]Indeed, Babuk Locker, a ransomware gang, announced in 2021 that it was closing its affiliate program and transitioning to an extortion-only model—stealing data and threatening to release it if payments were not

including DDoS attacks or efforts to publicize the attack or contact key customers or business partners.

Among other things, a business must evaluate whether it is obligated to provide notice of a security breach to consumers and regulators, as detailed in sections 27.08 and 27.09. Not every ransomware attack will require notification under U.S. law.

Ransomware attacks also may lead to regulatory enforcement by the Federal Trade Commission or State Attorneys' General and to litigation. Customers may seek indemnification or contributions where their businesses were impacted by a ransomware attack on a supplier. The victim itself also may have disputes with its insurer over coverage. In addition, consumers and shareholders may file putative class action suits, as analyzed in section 27.07. For these reasons, it is important for businesses to respond to ransomware attacks in coordination with counsel.[10]

A ransomware attack may also involve the theft of trade secrets which, if exposed, could destroy their value, as analyzed in chapter 10. Even if information does not rise to the level of a trade secret, its disclosure could cause competitive harm, put the victim in breach of third party obligations, or expose customer or employee information.

In responding to a ransomware attack, a company also should evaluate whether and when to involve law enforcement, which may provide useful information about a known attacker but may also discourage cooperation or payment of a ransom.[11]

While some ransomware attacks arise out of software flaws that are exploited by attackers, many have involved more

---

received—after concerns emerged about bugs in its decryptor program which could destroy the victim's files "and, potentially, lead to revenue losses for the gang in the future if victims' would've refused to pay ransoms." Segiu Gatlan, *Ransomware gang leaks data from Metropolitan Police Department,* Bleeping Computer, May 11, 2021. In addition to D.C. police personnel files, criminal case files and payroll data of the 63-officer Azusa, California police department were leaked online when the department refused to pay a ransom. *See* Harriet Ryan, *Ransomware hack puts sensitive Azusa Police Department documents online,* L.A. Times, May 31, 2021.

[10]*See supra* § 27.07[5] (preservation of privilege and confidentiality in putative data breach class action litigation).

[11]*See generally infra* chapter 43 (criminal vs. civil remedies and related considerations).

mundane methods to access a network such as using phishing emails to trick employees into opening an attachment or clicking on a link that downloads malware,[12] and thus can be countered by better employee training and vendor or other third party supervision. Businesses should also follow the periodic reports issued by the U.S. government's Cybersecurity & Infrastructure Security Agency, which reports on known attacks and the ways that a company may harden its protection against those attacks.[13]

The following checklist identifies ways that a business can mitigate its risk of a ransomware attack and outlines steps to take once an attack has occurred.

Planning in Advance

- Plan in advance to secure your systems and train employees, contractors and vendors to minimize the risk of a ransomware attack
- Adopt, implement, and update an incident response plan (which should anticipate alternative potential attacks)
- Obtain insurance
- Include a recovery strategy for dealing with ransomware attacks in a company's written information security or incident response plan
- Conduct tabletop exercises (including I.T., security,

---

[12] *See* Gerrit De Vynck, Rachel Lerman, Ellen Nakashima & Chris Alcantara, *The anatomy of a ransomware attack,* Wash. Post, July 9, 2021.

[13] CISA alerts are posted at https://www.cisa.gov/uscert/ncas/alerts. *See, e.g.,* CISA, *CISA, FBI, NSA and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities, available at* https://www.cisa.gov/news/2021/12/22/cisa-fbi-nsa-and-international-partners-issue-advisory-mitigate-apache-log4j (posted Dec. 22, 2021); CISA, *CISA, FBI, & NSA Release Joint Cybersecurity Advisory on BlackMatter Ransomware, available at* https://www.cisa.gov/uscert/ncas/current-activity/2021/10/18/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-blackmatter (posted Oct. 18, 2021); CISA, *CISA, FBI, & NSA Release Joint Cybersecurity Advisory on Conti Ransomware, available at* https://www.cisa.gov/uscert/ncas/current-activity/2021/09/22/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-conti (posted Sept. 22, 2021); U.K. National Cyber Security Centre, CISA, the U.S. Department of Justice & the NSA, Advisory, *Further TPPs Associated with SVR Cyber Actors*, *available at* https://www.ncsc.gov.uk/files/Advisory-further-TTPs-associated-with-SVR-cyber-actors.pdf (posted May 7, 2021).

Additional resources may be found at https://www.cisa.gov/stopransomware or StopRansomware.gov (which both resolve to the same location).

legal and communications professionals) to be ready to respond quickly when an attack occurs, directed by counsel

- Consider privilege issues to minimize the risk that a company's efforts to plan for ransomware attack become discoverable in litigation if an attack occurs[14]
- Retain offline mirror copies or complete backups of essential systems and data to minimize the risk of business interruption, and the likelihood that your company could be held hostage, in the event of an attack, and make sure that backups are current and operational[15]
- Plan in advance, to the extent possible, which lawyer(s) or consultants to use if negotiations are contemplated
- Implement and continually update industry standard security measures and best practices, as outlined elsewhere in this chapter, including using multi-factor authentication and avoiding or limiting use of accounts with administrative access privileges, where possible
- Train employees and audit vendor security to deter cybersecurity breaches and vulnerability to phishing scams
- Conduct regular vulnerability scans to identify and remediate vulnerabilities and regularly update and

---

[14]*See supra* § 27.07[5].

[15]The Cybersecurity & Infrastructure Security Agency recommended in mid-2020 that organizations:

- Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
- Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
  - — Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
- In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.

Cybersecurity & Infrastructure Security Agency and Multi-State Information Sharing & Analysis Center, Ransomware Guide 3 (Sept. 2020), *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

patch software, including antivirus and anti-malware software
- Audit contracts to verify if indemnification provisions would protect a company for an attack on a business partner, vendor or other third party, and consider whether to seek additional protection

When an Attack Occurs

- Determine what systems or information have been compromised and/or made inaccessible, isolate or shut down those components that have been compromised, and determine whether adequate backups or access exist to continue essential business functions
- Determine whether the attacker's access has been cut off or whether it is still able to access and compromise systems and data
- Consider coordination with law enforcement[16]
- Review CISA alerts on major ransomware attacks and evaluate if security researchers have available decryption tools since some Ransomware encryption algorithms have been broken
- Determine if there are notification requirements to consumers, state agencies, regulators, or business partners required by law[17] or contract
- Determine if trade secrets have been compromised[18]
- Evaluate if OFAC rules even allow for the payment of a ransom
- Even if paying a ransom is an option, consider whether restoration from a past backup would be a faster and more secure option

---

[16]*See generally infra* chapter 43. Among other things, reporting a ransomware attack to the appropriate U.S. government agency or agencies and cooperating with OFAC, law enforcement, and other relevant agencies, may be mitigating factors in the event of an OFAC violation. *See* U.S. Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* 5, Sept. 21, 2021, *available at* https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. A self-initiated and complete report of a potential violation will also be considered a mitigating factor. *See id*.

[17]*See supra* §§ 27.08, 27.09. Whether there is an obligation to provide notification may depend on whether information was exfiltrated or merely potentially accessible, and applicable state law. *See id.* Notification obligations may arise as quickly as 72 hours for EU consumers, under the GDPR. *See supra* § 26.04.

[18]*See supra* chapter 10.

- If a ransom deal is sought and may be lawfully made, identify the terms and objectives for an agreement, including confidentiality so publicity about a payment does not encourage further attacks, and consider using entities experienced in negotiating with ransomware attackers (such as Arete, Coveware and Kivu[19])
- Manage communications with employees, customers, vendors and others impacted by the attack
- Harden protection to prevent similar attacks in the future
- Evaluate whether indemnification obligations may be owed to the impacted business, to offset some of the costs

More specific recommendations on rebuilding compromised systems and technical best practices may be found in the Cybersecurity & Infrastructure Security Agency and Multi-State Information Sharing & Analysis Center's Ransomware Guide.[20]

---

[19]*See* Ellen Nakashima & Rachel Lerman, *Ransomware is a national security threat and a big business—and it's wreaking havoc,* Wash. Post, May 15, 2021. Negotiations "typically happen through email or an encrypted chat room on the 'dark web,' a portion of the Internet where sites are not accessible through search engines and typically require use of an anonymizing browser, like Tor." *Id.*; *see also* Rachel Monroe, *How to Negotiate with Ransomware Hackers,* New Yorker, May 31, 2021 (describing the experiences of Kurtis Minder of GroupSense).

[20]Cybersecurity & Infrastructure Security Agency and Multi-State Information Sharing & Analysis Center, Ransomware Guide (Sept. 2020), *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2023

Ian C. Ballon

2023 UPDATES – INCLUDING NEW AND IMPORTANT FEATURES

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator – a 5 volume-set & On Westlaw!

To order call 1-888-728-7677
or visit IanBallon.net

Key Features of E-Commerce & Internet Law

- AI, ML, screen scraping and data portability
- Antitrust in the era of techlash
- The CPRA, Virginia, Colorado and Nevada pricy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Software copyrightability and fair use after *Google v. Oracle*
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- The law of SEO and SEM – and its impact on e-commerce vendors
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi,* patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- Enforcing judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Applying the First Sale Doctrine to virtual goods
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Click fraud
- Copyright and Lanham Act fair use
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

Volume 1

Volume 2

Volume 3

Volume 4

Volume 5

"Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet."
Jay Monahan
General Counsel, ResearchGate

****

ABOUT THE AUTHOR

****

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2023, 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.lanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@lanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2023

- **Antitrust in the era of techlash** (chapter 34)
- **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurty breach, data privacy, AdTech and TCPA class action suits.**
- **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States,* 141 S. Ct. 1648 (2021)** (ch5)
- **FOSTA-SESTA** and ways to maximize CDA protection (ch 37)
- **IP aspects of the use of #hashtags** in social media (ch 6)
- The **CLOUD Act** (chapter 50)
- **Virginia, Colorado and Nevada privacy laws** (ch 26)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **Digital economy litigation strategies**
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- **Website and mobile accessibility** under the ADA and state laws (chapter 48)
- **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **AdTech law** (chapter 28, Darren Abernethy)
- **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- **eSIGN case law** (chapter 15)