H. Mark Lyon and Cassandra Gaedt-Sheckter

CCPA and the Dawn of Enforcement: Regulations, Global Privacy for the Future, and Where We Are Today

May 19, 2020

WHY NOW?

Why Now?

Enforcement period begins in six weeks—July 1, 2020

Confusing, variable time leading up to enforcement

- Late amendments
- Implementing regulations not yet final

Focus has been elsewhere

- Yet no delay on enforcement…

String of litigation has begun

BRIEF OVERVIEW OF CCPA

CCPA: An Overview

- CA residents get transparency into, and control over, how companies use and share their personal information.

- Will not be enforced until July 1, 2020

- Ever-evolving:
  - Amendments signed October 2019
  - AG's regulations threaten to broaden certain aspects (on third draft)
  - Consumer activists intend to overhaul with CCPA 2.0

CCPA: "Personal Information"

"Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"

IP addresses	*purchasing or consuming histories or tendencies*	browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement	biometric information

geolocation data	audio, electronic, visual, thermal, olfactory or similar information	*inferences drawn from any of this information*.

Cal. Civ. Code § 1798.140(o).

CCPA: Who Must Comply with the CCPA?

For-profit entities doing business in California that satisfy ***one*** or more of the following thresholds:

> **(A)** Annual gross revenues in excess of $25M
> **(B)** Deals with personal information of 50,000 or more consumers, households, or devices
> **(C)** Derives 50 percent or more of its annual revenues from selling personal information.
> *Cal. Civ. Code § 1798.140(c)(1).*

Despite not having typical "consumers," many businesses are covered if they have over $25M in annual gross revenue and do business in California.

CCPA: Rights of Californians

Understand what personal information is collected and why

Delete personal information, subject to exceptions

Access what personal information is **sold or shared**, and to/with whom

Opt out of the sale of their information (if consumer is under 16 years of age, must opt in)

Not be discriminated against for exercising any of these rights

CCPA: Rights of Californians – Reasonable Security

Section 1798.150 provides private right of action when "nonencrypted and nonredacted personal information" is subject to a breach "as a result of the business' violation of the duty to implement and maintain reasonable security procedures."

"Personal Information" defined narrower here (Section 1798.81.5(d)(1)(A)), California's existing data breach law (includes biometrics, SSN, IDs)

Potential Liability

- Breach provision expressly allows a private right of action: not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

- All other violations: civil action brought by the Attorney General with potential for "a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation." Up to seven thousand five hundred dollars ($7,500) for each intentional violation

CCPA DRAFT REGULATIONS

California Attorney General Regulations

Likely nearing final form

Three versions

- No. 1: October
- No. 2: February
- No. 3: March

Most recent deadline: March 27 (for comments)

California Attorney General Regulations

Notices need to be in plain language, accessible for disabled

Details regarding responding to requests (e.g., timing, ability to submit by two means, no webform)

No need to consider information maintained only for legal compliance

Service providers can use information for internal purposes so long as information is not used to augment other information/profiles

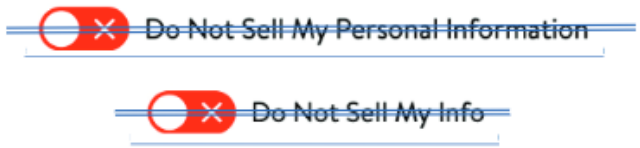
Record-keeping requirements for companies that use information from 4M-10M (e.g., number of requests)

California Attorney General Regulations

180° on personal information: “maintains [the] information in a manner that…”

Notice not required if not collected directly from consumer, and no sale

“Do Not Sell” Button Retracted



PRIVACY IN THE U.S. AND IMPLEMENTING A GLOBAL PRIVACY PROGRAM

Privacy Laws in the U.S.

Many have failed

- Washington state failed again, but passed facial recognition law
- Wisconsin bills (I) – (III)
- Mississippi

Others fall short of CCPA breadth

- Nevada – sale focus
- New York – SHIELD breach focus
- Maine – internet provider / advertiser focus

More proposals to come

- Federal privacy law – e.g., Data Protection Act
- COVID-19 Consumer Data Protection Act of 2020
- Washington state 4.0?

Global Privacy Program

Virtually impossible to do anything and please everyone

Consider a global-ish approach

- Consider where the business operates, and to what extent
- Find the common denominator
- Consider region-specific policies (e.g., EU, Asia, U.S.), country- or state-specific policies and procedures, when needed (e.g., consent, avoiding collection of certain data)

Operate with common privacy principles

- Transparency and choice: clear notice, and potentially, consent
- Minimize collection of information to what is needed
- Minimize usage to specific, defensible purpose
- Minimize storage and retention
- Ensure confidentiality and contractual protection if sharing with third parties
- Ensure security

CCPA COMPLIANCE: HOT BUTTON ISSUES

CCPA Compliance During COVID-19 and Other Hot Button Issues Likely to Spawn Litigation

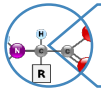
- COVID-19
- Compliance in 2021
- Large data breaches
- Data scrapers
- Sensitive information (minors / health)
- Biometrics

COVID-19 Management Programs Implicating CCPA


Internal modeling for reopening, prioritization of resources


Temperature screening


COVID-19 testing


Antibody (IgM/IgG) testing


Surveys, questionnaires, and other information gathering


Wearables, apps, and other contact tracing


WFH Vulnerabilities

COVID-19 Health Testing CCPA Concerns in More Detail

Notice

Exempted from personal information?

- Employment, B2B, HIPAA/CMI

Third parties/medical provider considerations

Incorporation into access/deletion request responses?

Security

Privacy best practices for context

- Limited collection and use
- Minimize retention, sharing

COVID-19 Contact Tracing in More Detail

Options for collection

- Proximity (GPS, Bluetooth, Wi-Fi?)
- What information?
  - Limited to close contact vs. retention of precise location
  - Aggregated / deidentified data – exempt?

Notice

Security

COVID-19 Brief Best Practices

- Consult with counsel, and encourage your business partners to consult with you.
  - Expanded definition of PII and new collections and uses of data mean expanded risks since initial CCPA compliance
  - Pandemic context can lead to moving too quickly
- When in doubt, transparency and consent rule
- Do not rely solely on public health, employment, or other guidance – need to consider CCPA
- Focus on reasonable security, particularly with WFH concerns

Compliance in 2021: What to Think About Now

Sunsetting provisions

- Employment-related information
- Business-to-business information

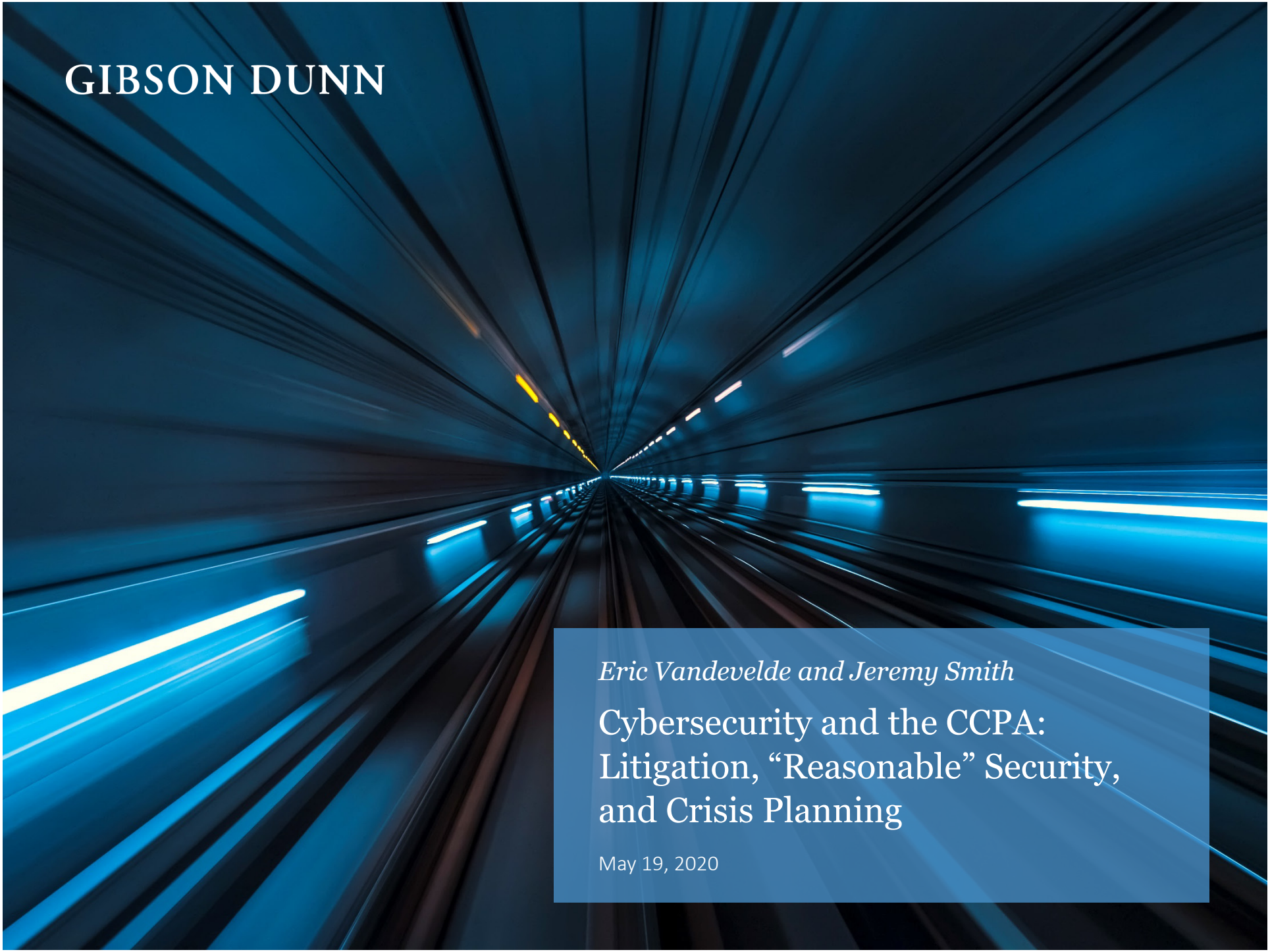
Updating policies (one year)

Close attention to litigation and enforcement actions

- Reasonable security in the new year

CCPA 2.0?

COVID-19 management, continued



Eric Vandevelde and Jeremy Smith

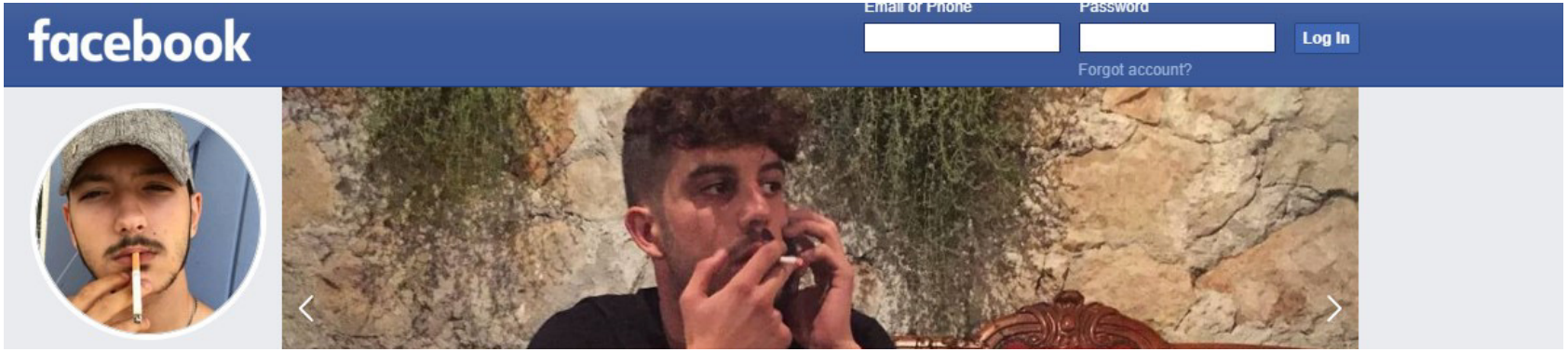
Cybersecurity and the CCPA: Litigation, "Reasonable" Security, and Crisis Planning

May 19, 2020

Some Questions for You

1. Has there been a privacy violation when a hospital unintentionally disclosed Dan's smoking status when there is a picture of him smoking on his public Facebook page?

2. Has there been an "egregious breach of the social norms" when a hospital unintentionally disclosed Dan's smoking status when there is a picture of him smoking on his public Facebook page?



The Common Law

- Breach of Contract, Intrusion upon Seclusion, Trespass, and Negligence
  - Generally requires proof of injury.
  - Generally requires proof of causation.
  - Often sets a high standard: e.g., an "egregious breach of the social norms."
- These common law claims are not well suited to class action litigation
  - Injury will often differ from individual to individual.
  - Causation will often differ from individual to individual.
  - Even the egregiousness of the breach will often differ from individual to individual.
- Plaintiffs have typically had more success with injunctive relief classes under Rule 23(b)(2).

A Question for You

Existing Statutes

- Most popular have been those with statutory damages.
  - Telephone Consumer Protection Act
  - Illinois's Biometric Information Privacy Act
  - California's Confidentiality of Medical Information Act
  - California Customer Records Act (statutory damages only for intentional acts)
- Others often invoked, even without statutory damages
  - California's Unfair Competition Law that provides for restitution and injunctive relief for unlawful, unfair, or fraudulent business acts or practices
  - FTC Act § 5 prohibits "unfair or deceptive practices in or affecting commerce." 15 U.S.C. Sec. 45(a)(1).
  - Video Privacy Protection Act (federal)
  - Stored Communications Act (federal)
  - California Consumers Legal Remedies Act

GIBSON DUNN

OVERVIEW OF CCPA

CCPA: Rights of Californians

Understand what personal information is collected and why

Delete personal information, subject to exceptions

Access what personal information is **sold or shared**, and to whom

Opt out of the sale of their information (if consumer is under 16 years of age, must opt in)

Not be discriminated against for exercising any of these rights

CCPA: Rights of Californians – Reasonable Security

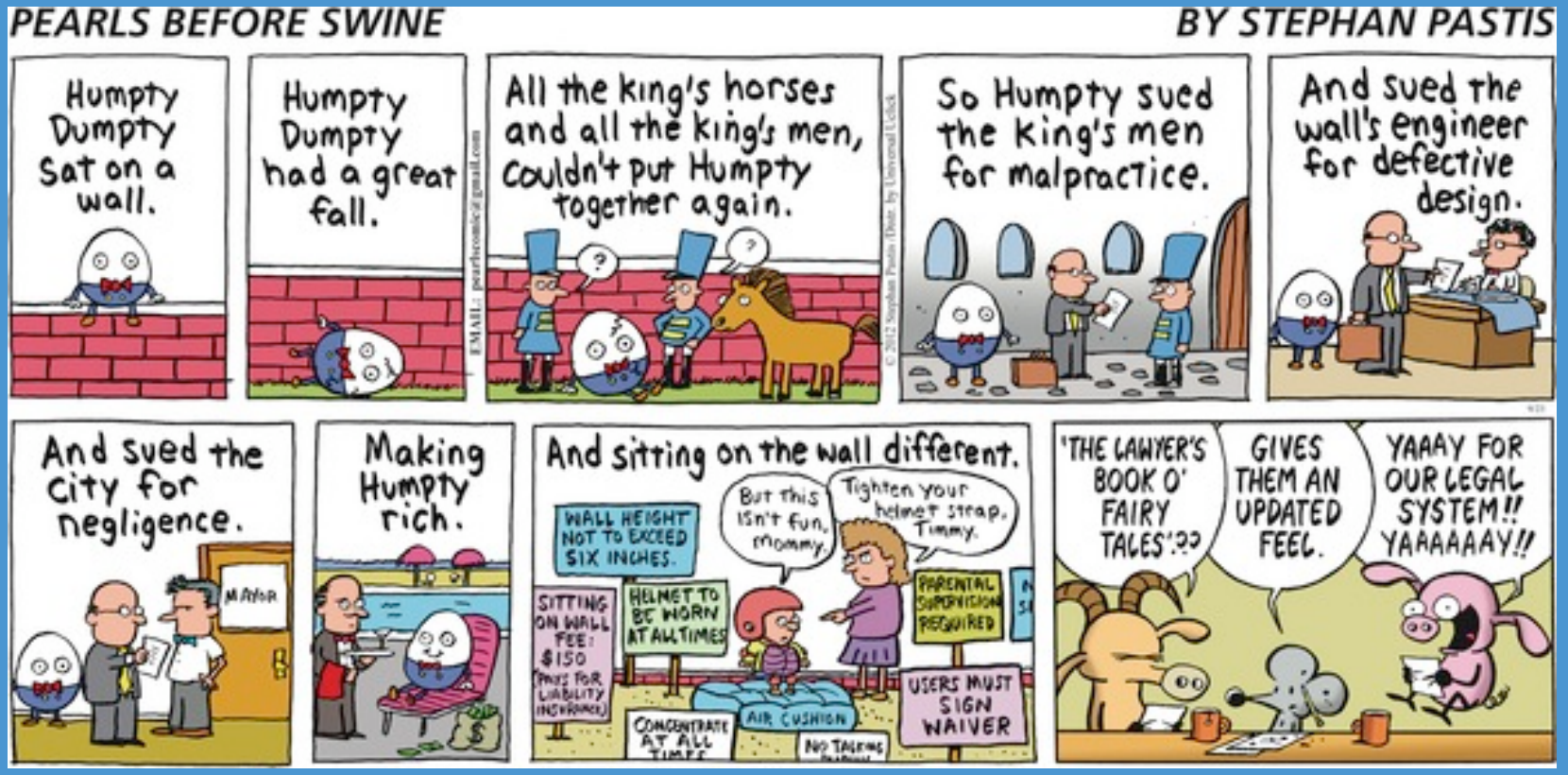
Section 1798.150 provides private right of action when "nonencrypted and nonredacted personal information" is subject to a breach "as a result of the business' violation of the duty to implement and maintain reasonable security procedures."

"Personal Information" defined narrower here (Section 1798.81.5(d)(1)(A), California's existing data breach law), and includes biometrics, SSN, IDs.

Potential Liability

- Breach provision expressly allows a private right of action: not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.
- All other violations: civil action brought by the Attorney General with potential for "a civil penalty of not more than $2,500 for each violation." Up to $7,500 for each intentional violation.
- UCL?
  - "Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Cal. Civ. Code § 1798.150(c)
  - Legislative Hx: "It appears that this provision would eliminate the ability of consumers to bring claims for violations of the Act under statutes such as the Unfair Competition Law, Business and Professions Code Section 17200 et seq. It also makes clear that the Act does not relieve any parties from having to follow the Constitution. This latter provision is likely unnecessary."

GIBSON DUNN



CLASS ACTIONS & AG ENFORCEMENT

The Wave Has Already Started

- *Burke v. Clearview AI, Inc.* (S.D.N.Y. No. 1:20-cv-03104).
  - Plaintiffs allege that "Clearview illicitly 'scraped' hundreds, if not thousands or more, websites, such as Facebook, Twitter, and Google, for over three billion images of consumers' faces."
  - Plaintiffs do not allege a CCPA claim directly based on allegations of collection and use without disclosure. Instead, they attempt to bootstrap it to a UCL claim.
- *Cullen v. Zoom Video Commc'ns Inc.* (N.D. Cal. No. 5:20-cv-02155-SVK) and Similar Cases.
  - *Hurvitz v. Zoom, Facebook, & LinkedIn* (C.D. Cal. No. 2:20-cv-03400); *Taylor* (N.D. Cal. No. 5:20-cv-02170); *Johnston* (N.D. Cal. No. 5:20-cv-02376); *Kondrat* (N.D. Cal. No. 5:20-cv-02520); *Lawton* (N.D. Cal. No. 5:20-cv-02592); *Jimenez*, (N.D. Cal. No. 5:20-cv-02591); *Hartmann* (N.D. Cal. No. 5:20-cv-02620); *Henry* (N.D. Cal. No. 5:20-cv-02691).
  - These putative class actions generally allege that Zoom wrongfully shared sensitive information with Facebook. Some also allege a lack of adequate encryption.
  - Some bring claims directly under the CCPA; others bootstrap to the UCL.

The Wave Has Already Started

- *Barnes v. Hanna Andersson & Salesforce* (N.D. Cal. No. 3:20-cv-00812-DMR)
  - The plaintiff alleges that "[h]ackers not only 'scraped' many of Hanna's customers' names from the website [hosted by Salesforce] by infecting it with malware, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates."
  - The complaint alleges violations of the UCL and the CCPA's data breach provision, § 1798.150, which provides for a private right of action for "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."
  - The complaint also brings a negligence claim.
  - Retroactive? Can a plaintiff bring a CCPA claim based on events that predate the law going into effect on January 1?

Sleight of Hand?

- The CCPA was sold as a compromise because the private right of action was for "data breaches" and the law specifically prevents bootstrapping to the UCL.
  - "Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: …." Cal. Civ. Code § 1798.150(a)(1).
    - Do the *Clearview*, *Zoom*, and *Hanna Anderson* cases fit? Are they data breaches?
  - "Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Cal. Civ. Code § 1798.150(c).

Key Provisions for Defendants

- Section 1798.150 only provides a remedy if the business violated its "duty to implement and maintain ***reasonable security procedures and practices*** appropriate to the nature of the information to protect the personal information."
  - Litigants often look to outside sources for validation, e.g.,:
    - National Institute of Standards and Technology
    - Payment Card Industry Data Security Standard (PCI DSS)
    - FedRAMP (standardized approach to cloud security)
    - CIS Critical Security Controls
    - ISO 27001
    - FTC guidance
    - SEC guidance
    - CFPB guidance
    - AG guidance

Will courts look to GDPR for what constitutes "***reasonable security procedures***"?

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
   a) the pseudonymisation and encryption of personal data;
   b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

   (Art. 32 GDPR)

Will Courts look to other U.S. Laws?

HIPAA's Security Rule: covered entities must:

(1) ***Standard: Access control.*** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) ***Unique user identification (Required).*** Assign a unique name and/or number for identifying and tracking user identity.

(ii) ***Emergency access procedure (Required).*** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) ***Automatic logoff (Addressable).*** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) ***Encryption and decryption (Addressable).*** Implement a mechanism to encrypt and decrypt electronic protected health information

....

Do you follow cybersecurity norms and best practices? How do you stack up to others?

- What kind of record can you make? Can you show the company took cybersecurity seriously?
  - Corporate governance – Cybersecurity expertise on board? Training? Which board committee oversees? Regular meetings? What is reported? Do you have a CISO and CPO?
  - Data mapping – Do you know what data you have? What are the crown jewels? Do you encrypt what you can? Do you delete what you don't need?
  - Risk assessments – What are your trends? Can you show improvement? What are your benchmarks? What guidance are you following?
  - Technical controls – e.g., IDS, DLP, malware, anti-virus, phishing email detection
  - Incident response plan and other policies – Is it "just an IT thing" at your company? Are you getting the low-hanging fruit? Strong passwords, appropriate access control/permissions, etc.?
  - Information sharing – do you know what your primary threats are?
  - Resources – Are they enough? Would your CISO/CPO agree?
  - Feedback loop – What have you done for me lately? Standing still = failure.

How Much Protection Does the "Reasonable" Standard Provide?

- Battle of the experts
  - The CISO
  - Former Law Enforcement
  - Former Cybercriminal
  - E-discovery Expert
- Problems of Monday-morning quarterback
- Emails from IT and cybersecurity professionals
- Technical debt
- Insider threats
- Moving goalposts

Key Provisions for Defendants

- Section 1798.150 only applies if the information was "*nonencrypted* and *nonredacted*."
  - Does not appear to require any level or type of encryption.
  - This could make the law outdated quickly.

Key Provisions for Defendants

- Section 1798.150 only applies if the information was "personal information."
  - And as mentioned earlier, it's a narrower definition: "first name or first initial and the individual's last name in combination with" a " Social security number," "Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual," an "[a]ccount number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account," "[m]edical information," "[h]ealth insurance information," or "[u]nique biometric data." Cal. Civ. Code § 1798.81.5(d)(1)(A).
  - There may also be a "real" requirement: "Personal Information" includes "[i]dentifiers such as a *real* name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers." Cal. Civ. Code § 1798.140(o)(1)(A) (emphasis added).

Hypo Time!

- A national retailer was the victim of an easily avoided malware intrusion. Robert "Bob" Smith was a customer, and in the exposed database it had "B. Smith," his credit card number, and his zip code. This information was available to the criminals who successfully executed the malware attack, and now is available to the international criminal syndicate that purchased the whole data dump for $20,000 worth of Bitcoin. Bob's credit card number expired 2 years ago and Bob is now deceased. Did Bob have personal information exposed such that he may have a claim under § 1798.150?

Where We Expect These Cases to Be Decided

- Motion to Dismiss
  - Article-III-no-injury arguments led to the dismissal of many of the early privacy class actions:
    - The court *In re Specific Media Flash Cookies Litigation*, Case No. 10-1256, 2011 U.S. Dist. LEXIS 50543 (C.D. Cal. Apr. 28, 2011) held no Article III standing in a case involving the alleged use of "Flash cookies" by an online advertising network to track Internet users without their knowledge or consent.
    - The court *in In re iPhone Application Litigation*, Case No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865 (N.D. Cal. Sept. 20, 2011) dismissed a privacy class action on Article III grounds in the mobile device context.
    - The Ninth Circuit in *Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 722, 724 (9th Cir. 2017) affirmed the dismissal on Article III standing grounds of a putative class action alleging Toyota's cars had a "hacking" vulnerability.
    - The court in *Antman v. Uber Techs., Inc.*, No. 15-CV-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) held no Article III standing in a putative class action involving a breach of Uber's driver information.
  - But courts have begun to hold that data breaches and privacy violations inherently cause people injury by increasing the risk of identity fraud, which is sufficient to support Article III standing.

Where We Expect These Cases to Be Decided

- Class Certification
  - This is the trial in data privacy class actions.
    - No significant data privacy class action has progressed past class certification.
      - Yahoo settled within days of the filing the opposition to class certification.
      - Anthem also settled while litigating class certification.
    - Nearly every contested class certification has resulted in denial of Rule 23(b)(3) certification.
      - *E.g., Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 699 (N.D. Cal. 2019) (denied 23(b)(3) certification; granted 23(b)(2) certification); *S. Indep. Bank v. Fred's, Inc.*, No. 2:15-CV-799-WKW, 2019 WL 1179396 (M.D. Ala. Mar. 13, 2019) (denied); *Dolmage v. Combined Ins. Co. of Am.*, 2017 WL 1754772, at *7 (N.D. Ill. May 3, 2017) (denied); *but see Smith v. Triad of Alabama, LLC*, 2017 WL 1044692 (M.D. Ala. Mar. 17, 2017).
    - But those were nearly all cases *without* statutory damages.

Where We Expect These Cases to Be Decided

- How to Defeat Class Certification
  - Must *prove*, not just as a theoretical matter, but with overwhelming evidence, that the case cannot proceed as a class action.
    - Leverage your "exposed" data. Don't assume it's uniform. It's probably not. How many Smiths do you have? How many putative class members are named Jane Doe and Bruce Wayne?
    - Leverage the public record: social media, voting rolls, etc.
    - Leverage differences in your named plaintiffs.
    - If possible, show that "common issues" impact some individuals differently.
    - Focus on unique affirmative defenses of named plaintiffs *and* certain class members
    - Are you willing to say *some* class members may have valid claims?

Individual Inquiries for Statutory Damages?

- To determine whether to award $100, $750, or somewhere in between, the court should consider, among other factors, "***the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct***, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." Cal. Civ. Code § 1798.150(2) (emphasis added).
- The first three factors will often depend on the individual. For example, new customers will often be in a very different position than very old customers. A brand new customer, for example, may have had little information exposed and for a very short time in comparison to other customers, and thus per the statute must receive less.
- There is also a good argument that courts must examine the "*actual or potential harm suffered by the plaintiff*" to ensure the award does not offend Due Process. *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 418 (2003); *St. Louis, I.M. & S. Ry. Co. v. Williams*, 251 U.S. 63, 67 (1919).
- This strategy has support from analogous situations: e.g., *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 269 (N.D. Cal. 2016).

The PR Strategy & Litigation Strategy Intersect

- Public Relations Efforts Can Both Help and Hurt Litigation Strategy.
  - Both in the press and in court, the narrative is critical.
    - The "killer" legal argument that minimizes the importance of everyone's data will likely backfire in both the press and the court.
    - Craft the narrative to fit the company's brand and image.
  - Early responses can be very harmful
    - Categorical statements about the data.
    - Statements that later could seem like the company was downplaying or misleading.
  - Early responses can also be very helpful
    - Class actions typically follow news coverage.
    - Limiting the news coverage will often limit the potential for numerous class actions.
    - It may also limit the interest of government entities.

Which One Do You Like Best?

1. "We have fixed the issue and informed customers who may have been impacted." "[The Company] takes all security-related matters very seriously and your account security is our top priority. We have policies and security measures in place to ensure that your personal information remains secure."
2. "The investigation has confirmed that [the company's] platform was infected with malware that may have scraped information entered by customers into the platform."
3. "[We] were the target of a very sophisticated external cyber attack." "These attackers gained unauthorized access to [the] IT system and have obtained personal information from our current and former members, such as their names, birthdays, medical IDs/social security numbers, street addresses, e-mail addresses and employment information, including income data."

The Role of the Attorney General

- Unclear at this point.
- The AG has announced enforcement will not begin until July 1, 2020
- The AG will likely focus on the notice and consent provisions that are not obvious candidates for private actions under § 1798.150.

The Attorney General's Hammer

- Civil penalty of not more than $2,500 "for each violation."
- If intentional → $7,500 "for each intentional violation."
- Business shall be in violation "if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance."

Cal. Civ. Code § 1798.155.

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2001 Ross Avenue, Suite 2100
Dallas, TX 75201-2923
+1 214.698.3100

Denver
1801 California Street
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 370 0311

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
1221 McKinney Street
Houston, TX 77010
+1 346.718.6600

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
166, rue du faubourg Saint Honoré
75008 Paris
France
+33 (0)1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35°andar
Sao Paulo 04551-060
Brazil
+55 (11)3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500