NOSSAMAN LLP

# SUMMARY OF SELECTED CALIFORNIA PRIVACY LAWS

**NOSSAMAN LLP**

**THOMAS DOVER**

**STEPHEN P. WIMAN**

**March 2019**

# CONTENTS

# INTRODUCTION

Title 1.81 of Part 4, Division 3 of the Civil Code, contains sections relevant to privacy and the handling of "customer" information. This summary discusses four of those sections: 1798.81.5 (reasonable security of personal information); 1798.82 (disclosure of a data breach involving personal information); 1798.83 (Shine the Light Law – disclosures regarding a business sharing a customer's personal information with a third party) and 1798.84 (remedies for violation of provisions of Title 1.81).

# CIVIL CODE SECTION 1798.81.5

## (Reasonable Security Of Personal Information)

Section 1798.81.5(b) of the Civil Code requires "[a] business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

"[T]he terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." (Civ. Code, § 1798.81.5(a)(2).) "Maintain" includes personal information a business maintains but does not own or license. (*Ibid.*)

Additionally, any business that discloses personal information about a "California resident" pursuant to a contract with a nonaffiliated third party that is not subject to subdivision 1798.81.5(b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code, § 1798.81.5(c).)

Section 1798.81.5(d) defines "personal information as:

> **(1)** "Personal information" means either of the following:
>
> (A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
>
> (i) Social security number.

> (ii) Driver's license number or California identification card number.
>
> (iii) Account number, 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.
>
> (iv) Medical information.
>
> (v) Health insurance information.
>
> (B) A username or email address in combination with a password or security question and answer that would permit access to an online account.
>
> (2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.
>
> (3) "Health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
>
> (4) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Section 1798.81.5(e) excludes from the section certain information covered by other referenced sections of the California Codes and federal law such as California's Confidentiality of Medical Information Act and Health Insurance Portability and Availability Act ("HIPAA"). (See *Fero v.*

*Excellus Health Plan, Inc. (*W.D.N.Y. 2017) 236 F.Supp.3d 735, 782 [applying the exclusion of California's Confidentiality of Medical Information Act].) Lastly, section 1798.81.5(e)(5) provides that for businesses regulated by a stricter state or federal statute, compliance with that stricter standard is compliance with section 1798.81.5.)

A violation of this section is subject to section 1798.84 of the Civil Code regarding violations and remedies. (Civ. Code, § 1798.84(b) ["Any customer injured by a violation of this title may institute a civil action to recover damages."].)

**Questions/Comments:**

Note that the section does not define further "reasonable security procedures and practices."

The section also does not define "nonaffiliated third party."

The section expressly applies to "California residents." Does the statute require that a complaining party be a "customer?" One court has ruled that one must be a customer in order to have standing in federal court. (*Thibodeau v. ADT Security Service* (S.D.Cal. April 16, 2018, 3:16-cv-02680-GPC-AGS) 2018 U.S.Dist. Lexis 63888, *10-*11; *Thibodeau v. ADT Security Service* (S.D.Cal. Jan. 31, 2018, 3:16-cv-02680-GPC-AGS) 2018 U.S.Dist. Lexis 16094, *17-*19.) Note that the remedial section Civil Code section 1798.84(b) refers to "customer."

The definition of "personal information" in the section is the definition of "personal information" under section 1798.150 of the Civil Code (private enforcement of the California Consumer Privacy Act).

# CIVIL CODE SECTION 1798.82

**(Disclosure Of A Data Breach Involving Personal Information)**

Section 1798.82(a) of the Civil Code requires a person or business

> that *conducts business in California*, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose *unencrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose *encrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

(Emphasis added.)

Section 1798.82(a) also requires that the disclosure must be made in the most expedient time possible and without unreasonable delay, "consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

If a person or business "maintains" data but does not own it, the person or business must notify the owner or license of the data of a breach. (Civ. Code, § 1798.82(b).)

Section 1798.82(d) sets forth a very specific and lengthy list of steps for the person or business to take in order to provide notification of the breach. A written notice is required and is to include information, inter alia, of what happened, what information was involved, what is being done and what the person whose information is breached can do.

If notification to more than 500 persons is required, the person or business experiencing the breach must submit a sample copy of the security breach notification to the Attorney General.

Section 1798.82(g) defines "breach of security of the system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

Section 1798.82(h), in defining "personal information," mirrors Section 1798.81.5(d), quoted above.

# CIVIL CODE SECTION 1798.83

**(Shine The Light Law – Disclosures Regarding A Business Sharing A Customer's Personal Information With A Third Party)**

Section 1798.83 of the Civil Code is sometimes identified as the "Shine the Light Law." This section is intended to make clear what a business's information sharing practices are with third parties. *E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition* (2019), summarizes the section as follows:

> Section 1798.83 provides that if a business with twenty or more full or part-time employees has an *established business relationship* with a *customer* and has within the immediately preceding calendar year *disclosed* specified categories of *personal information* (or certain information derived from this information) to *third parties*, and if the business knows or reasonably should know that the *third parties* used the *personal information* for their own *direct marketing purposes*, the business shall, upon request once per calendar year, provide the *customer* free of charge (in writing or by email) within thirty (30) days:
>
> • a list of the categories disclosed for *third party direct marketing purposes* during the immediately preceding calendar year; and
>
> • the names and addresses of all of the *third parties* that received such information and, if the nature of the *third parties'* business cannot reasonably be determined from their names, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.

> The obligations under this statute may be avoided if a business otherwise required to comply with the statute (1) adopts and discloses to the public in its privacy statement a policy of not disclosing *personal information* of customers to third parties for the *third parties' direct marketing purposes* unless the *customer* first affirmatively agrees to that disclosure, or of not disclosing such information if the *customer* has "exercised an option that prevents that information from being disclosed to *third parties* for those purposes," (2) maintains and discloses this policy, (3) notifies the *customer* of his or her right to prevent disclosure of *personal information*, and (4) provides the *customer* with a cost free means to exercise this right.
>
> In other words, a business subject to the statute must do one of the following: (1) refrain from *third party* transfers; (2) adopt and disclose a policy of requiring opt-in consent for *third party* transfers; (3) adopt and disclose a policy of allowing consumers to opt-out of *third party* disclosures; or (4) allow [customers] to obtain an annual written disclosure, upon request, of *third party* transfers.

(I. Ballon, *E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition* (2019) Ch. 26, § 26.13[6][D], footnotes omitted, emphasis added; see Civ. Code, § 1798.83(a) and (c)(2) and 15 U.S.C. § 6803.)

> [S]ubdivision (b) requires businesses to designate a mailing address, e-mail address, telephone number, or facsimile number where customers may send disclosure requests, and it requires businesses to advise customers of the designated addresses or telephone numbers in at least one of three ways: (1) notify managers who supervise employees who

> regularly interact with customers of the designated addresses and phone numbers and instruct those employees that customers who inquire shall be informed of the addresses or phone numbers; (2) add to the home page of its Web site a link either to a page titled "Your Privacy Rights" or add the words "Your Privacy Rights" to the home page's link to the business's privacy policy; the first page of the link "shall describe a customer's rights pursuant to this section and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate"; or (3) make the designated addresses or phone numbers readily available upon request of a customer at every place of business in California where the business or its agents regularly have contact with customers. (§ 1798.83, subd. (b)(1).) Responses to disclosure requests must be provided within 30 days. (§ 1798.83, subd. (b)(1)(C).)

(*Boorstein v. CBS Interactive, Inc.* (2013) 222 Cal.App.4th 456, 464; see discussion of Civil Code section 1798.84 and *Boorstein* in the next section relating to standing to pursue a claim under section 1798.83.)

The court in *Boorstein* described the purpose of section 1798.83 as follows:

> According to its legislative history, the STL law was intended to "provide consumers with information on how their information is being shared by companies." (Sen. Com. on Judiciary, Analysis of Sen. Bill No. 27 (2003–2004 Reg. Sess.) as amended Apr. 30, 2003, p. 1.) The bill's author said that at the time of the STL law's enactment, consumers were not only unable to stop the buying and selling of their personal information, "they do

> not even know whether and to what extent it is taking place … .” (Sen. Com. on Judiciary, Analysis of Sen. Bill No. 27 (2003–2004 Reg. Sess.) as amended Apr. 30, 2003, p. 3.) The STL law, thus, “is designed to let market forces work by shining light on [businesses' ]information sharing practices” so consumers can make educated privacy decisions and knowledgeable marketplace decisions. (Sen. Com. on Banking and Finance, Analysis of Sen. Bill No. 27 (2003–2004 Reg. Sess.) as amended July 2, 2003, p. 5.)

(*Id*. at p.465.)

The statute defines the italicized words, among others: *customer*; *direct marketing purposes, disclosed*; *established business relationship*; *personal information*; *third parties*. (Civ. Code, § 1798.83(e)(1), (2), (3), (5), (7) and (8).)

Section 1789.83(e)(1) defines “customer” as “an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an *established business relationship* if the business relationship is primarily for personal, family, or household purposes.”

Section 1798.83(e)(2) defines “direct marketing purposes, with certain exceptions as the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes.” The sale of personal information for consideration to businesses also can be a direct marketing purpose.

Section 1798.83(e)(5) defines “established business relationship” to include, among other criteria, a relationship formed by a voluntary, two-way communication between a business and customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal property. . . or obtaining a product or service . . . .”

In two lengthy lists, section 1798.83(e)(6) and (7), respectively, define "categories" of personal information required to be disclosed and "personal information" itself.

Finally, section 1798.83(e)(8) defines "third party" as any one of three alternatives:

(1) A business that is a separate legal entity from the business that has an *established business relationship* with a *customer*;

(2) A business that has access to a shared database if the business is authorized to use the database for *direct marketing purposes* unless the use of the database is exempt from being considered a *disclosure* not for *direct marketing purposes* under section 1798.83(d); or

(3) A business not affiliated by a common ownership or common corporate control with the business required to comply with the statute.

Certain disclosures between affiliated third parties that share the same brand are exempt from the requirements of the statute. (Civ. Code, § 1798.83(f).)

Section 1798.83(d) provides a long list of specific disclosures not subject to the statute. This section should be examined to determine whether a particular business, in the context of the disclosure at issue, is exempt.[1]

**Questions/Comments:**

Note that the section applies to information of "customers," not a broader category of "California residents" as does the California Consumer Privacy Act.

---

[1] One example of an exemption is the circumstance where a business discloses to a *third party* under a contract or arrangement where the *third party* processes, stores, manages, or organizes *personal information* where the *third party* does not use the information for its own *direct marketing purposes.*

Regarding an annual written disclosure under 15 U.S.C. § 6803, is a customer entitled to prevent disclosure to a third party?

# CIVIL CODE SECTION 1798.84

## (Remedies For Violation Of Provisions Of Title 1.81)

Section 1798.84 of the Civil Code provides remedies for violations of Title 1.81 of Part 4 of Division 3 of the Civil Code which includes sections 1798.80 through 1798.84. As an initial matter, under section 1798.84(a), any waiver of a provision of Title 1.81 is contrary to public policy and is void and unenforceable.

Section 1798.84 provides that "[a]ny customer injured by a violation of this title may institute a civil action to recover damages." Additionally, "[a]ny business that violates, proposes to violate or has violated this title may be enjoined." (Civ. Code, § 1798.84(e); see *Hameed-Bolden v. Forever 21 Retail, Inc.* (C.D.Cal. Oct. 1, 2018, No. 18-03019 SJO (JPRx)) 2018 U.S.Dist. 217868 , *19-*20 [cause of action stated under section 1798.84 for alleged violation of section 1798.81.5 for failure to maintain reasonable security procedures and practices]; *In re Sony Gaming Networks & Customer Data Security Breach Litigation* (S.D.Cal. 2014) 996 F.Supp.2d 942, 1010 [cause of action stated for injunctive relief, not economic damages, for violation of section 1798.82].)

Specifically regarding section 1798.83, a *customer* may recover a civil penalty of up to $3,000 per each willful, intentional or reckless violation of that section. For a non-willful, unintentional or non-reckless violation of the section, the customer may recover a civil penalty of up to $500 per violation. (Civ. Code, § 1798.84(c).) A prevailing plaintiff suing for a violation of section 1798.83 "shall also be entitled to recover his or her reasonable attorney's fees and costs." (Civ. Code, § 1798.83(g).)

Section 1798.84(d) provides a safe harbor to a business:

> **(d)** Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information

> required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

Lastly, section 1798.84(f)(1) exempts a business from liability for disposing of abandoned records containing *personal information* by shredding, erasing or otherwise modifying the *personal information* in the records to make it unreadable or undecipherable. By this section, "[i]t is the intent of the Legislature in paragraph (1) to create a safe harbor for such a record custodian who properly disposes of the records in accordance with paragraph (1)." (Civ. Code, § 1798.84(f)(2).)

In *Boorstein v. CBS Interactive, Inc.* (2013) 222 Cal.App.4th 456, the Court of Appeal held that a plaintiff did not have standing under sections 1798.83 and 1798.84 to sue where the plaintiff did not, and could not, allege that he had made a disclosure request under section 1798.83(a). According to the court, the plaintiff had not suffered any injury as a result of a violation of the statute. In reaching this holding, the court cited the following cases with similar holdings: *Murray v. Time Inc.* (N.D.Cal. Aug. 24, 2012, No. C 12-00431 JSW)) 2012 U.S.Dist. Lexis 120150; *Miller v. Hearst Communications, Inc.* (C.D.Cal. Aug. 3, 2012, No. CV 12-0733-GHK (PLAx)) 2012 U.S.Dist. Lexis 109121; *King v. Conde Nast Publications* (C.D.Cal. Aug. 3, 2012, CV 12-0719-GHK (Ex)) 2012 U.S.Dist. Lexis 109120; *Boorstein v. Men's Journal LLC* (C.D.Cal. June 14, 2012, No. CV 12-7771 (Ex)) 2012 U.S.Dist. Lexis 83101.

**Questions/Comment:**

Regarding *Boorstein v. CBS Interactive, Inc.*, the plaintiff therein argued that failure to comply with any provision of section 1798.83 constitutes an actionable violation. The court rejected the argument and held that the plaintiff had no cause of action for violation of the statute. This was all in the context of the plaintiff seeking statutory damages. Query whether had the plaintiff been seeking injunctive relief against a violation of the statute (e.g. failure to comply with posting requirements), the court would have concluded that he did not have standing. (See, e.g., *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, *supra*, 996 F.Supp.2d 942, 1010 [plaintiffs could pursue injunctive relief for alleged violation of section 1798.82 under section 1798.84 even though they had no standing to pursue economic damages]; cf. *Murray v. Time Inc., supra*, 2012 U.S.Dist. Lexis 120150 at pp. *18-*19 [no standing for injunctive relief].)

# BUSINESS AND PROFESSIONS CODE SECTIONS 22575 ET SEQ.

## (Online Privacy Protection Act Of 2003)

The California Legislature enacted the Online Privacy Protection Act of 2003, Stats. 2003, ch. 829, with the following findings and declarations:

> The Legislature finds and declares all of the following:
>
> (a) Each operator of a commercial Web site or online service has an obligation to post privacy policies that inform consumers who are located in California of the Web site's or online service's information practices with regard to consumers' personally identifiable information and to abide by those policies.
>
> (b) It is the intent of the Legislature to require each operator of a commercial Web site or online service to provide individual consumers residing in California who use or visit the commercial Web site or online service with notice of its privacy policies, thus improving the knowledge these individuals have as to whether personally identifiable information obtained by the commercial Web site through the Internet may be disclosed, sold, or shared.
>
> (c) It is the intent of the Legislature that Internet service providers or similar entities shall have no obligations under this act related to personally identifiable information that they transmit or store at the request of third parties.

(Stats. 2003, ch. 829, § 2.)

Under the act, a commercial Web site *operator*/online service that collects *personally identifiable information* from California resident *consumers* who use or visit the site or service must *conspicuously post* its privacy policy on the Web site or, in the case of an online service, use any reasonably accessible means of making the policy available for consumers of the service. (Bus. & Prof. Code, § 22575(a) and 22577(b); see *Apple Inc. v. Superior Court* (2013) 56 Cal.4th 128, 147 [discussing statute].) Section 22677(b) describes in detail various alternative methods for "conspicuously posting" the privacy policy.

An operator is in violation of its posting obligation only if the operator fails to post its policy within 30 days after being notified of noncompliance. (Bus. & Prof. Code, § 22575(a).)

In addition to identifying its effective date, the privacy policy must do all of the following:

> (1) Identify the categories of *personally identifiable information* that the *operator* collects through the Web site or online service about individual *consumers* who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that *personally identifiable information*.
>
> (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
>
> (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material

> changes to the operator's privacy policy for that Web site or online service.

(Bus. & Prof. Code, § 22575(b).)

Section 22577 also defines the italicized terms above: "personally identifiable information" (§ 22577(a)); "operator" (§ 22577(c)); and "consumer" (§ 22577(d)).

*Personally identifiable information* includes "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:" a first and last name; a home or other physical address, including street name and name of a city or town; an e-mail address. a telephone number; a social security number; any other identifier that permits the physical or online contacting of a specific individual; or Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with another identifier described above.

*Operator* includes a person or entity that owns a Web site located on the Internet or an online service operated for commercial purposes that collects and maintains *personally identifiable information* from a California resident *consumer*. *Operator* "does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner."

A *consumer* is any individual "who seeks or acquires, by purchase or lease, any goods, services, money or credit for personal, family, or household purposes."