The scope of the CCPA's Private Right of Action may be expanded

The impact of this right may go further than just data breach cases. By **Simon Frankel**, **Cortlin Lannin**, **Kathryn Cahoy** and **Rafael Reyneri** of Covington & Burling.

The California Consumer Privacy Act (CCPA) is the first comprehensive privacy law of its kind in the United States. While the California Attorney General has sweeping enforcement power under the law, the private right of action in the CCPA is much more limited in scope. Nevertheless, since the law went into effect on 1 January 2020, several private plaintiffs have asserted claims under the CCPA, some seemingly seeking to expand the private right of action. This article analyzes certain trends reflected in these actions.

The CCPA's limited private right of action

Although the CCPA contains a wide-ranging set of requirements, most cannot be enforced through the CCPA's private right of action. That provision authorizes private civil suits only for consumers "whose nonencrypted and nonredacted personal information, as defined [by the California data breach law], 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 ... ." Cal. Civ. Code § 1798.150(a)(1). Put another way, a claim brought under the CCPA's private right of action must satisfy four elements:

1. Personal information, as defined in the California data breach law;
2. was subject to unauthorized access and exfiltration/theft/disclosure;
3. in a nonencrypted and nonredacted form; and
4. the access and exfiltration/theft/disclosure resulted from the defendant's failure to implement and maintain reasonable security procedures and practices.

The CCPA thus expressly limits the private right of action in three important ways. First, the statute allows a private right of action only for claims that meet the requirements delineated in section 1798.150(a) – not for other violations of the CCPA. Second, the private right of action incorporates the California data breach statute's narrower definition of personal information, rather than the CCPA's more expansive definition. Third, the statute provides that "[n]othing in [the CCPA] shall be interpreted to serve as the basis for a private right of action under any other law."

Private plaintiffs who fall within the narrow confines of this private right of action may recover actual damages, injunctive relief, and statutory damages of up to $750 per consumer "per incident." Before filing a claim for statutory damages, plaintiffs must provide businesses with 30 days to rectify the alleged violation. If a business is able to rectify within 30 days and provides the plaintiffs with notice of the rectification, no action for statutory damages (whether on an individual or class basis) may be brought.

Private plaintiffs test the boundaries

Since the CCPA went into effect on 1 January 2020, private plaintiffs have begun filing complaints that include claims under the CCPA or otherwise invoke the CCPA. Some of these claims seem to fit within the CCPA's private right of action while others would, if allowed to go forward, seem to expand the scope of the private right of action.

Several CCPA claims have arisen from alleged data breaches. For example, cloud software provider Blackbaud suffered a ransomware attack that has spurred multiple lawsuits. In *Estes v. Blackbaud,* No. 20-cv-8275 (C.D. Cal. filed 9 Sept. 2020), the plaintiff invokes the CCPA private right of action (in addition to various common law claims), contending that Blackbaud violated the CCPA by failing to maintain reasonable security practices to prevent the theft and disclosure of the plaintiff's personal information. Other reported data breaches, for example the one involving Hanna Andersson, have resulted in similar CCPA claims. See *In re Hanna Andersson Data Breach Litigation*, No. 20-cv-812 (N.D. Cal. filed 3 Feb. 2020).

The claims set forth in these cases fall within the confines of the direct private right of action under the CCPA and thus do not threaten to significantly expand the outer bounds of the CCPA's private right of action. However, the cases may provide opportunities for courts to clarify certain ambiguities in the statute, including what constitute reasonable security measures. In addition, these cases may provide initial signals regarding the expected settlement value associated with data breaches now that the CCPA has gone into effect. *In re Hanna Andersson*[1], for example, has been stayed pending settlement negotiations and may provide insight on this front if the parties reach a class-wide settlement that must be publicly filed and approved by the court.

Other plaintiffs, however, appear to be attempting to expand the scope of the CCPA's private right of action by asserting direct CCPA claims that are not related to data breaches. For example, in *Sweeney v. Life on Air*, No. 20-cv-742, (S.D. Cal. filed 17 Apr. 2020), the plaintiff alleged that a social networking app, Houseparty, collected the personal information of its users and disclosed that information to third parties without user permission. The complaint asserts a claim under the CCPA based on alleged violations of the statute's provisions related to notice (§ 1798.100(b)), opt-out (§ 1798.120(b)), and the "Do Not Sell" button (§ 1798.135(a)). Despite seeking to enforce the CCPA directly, the plaintiff does not mention the standard for a CCPA private right of action articulated in California Civil Code section 1798.150(a) and does not attempt to explain how the violations

were caused by lack of reasonable security procedures. Given the CCPA's statutory text limiting the private right of action to section 150(a), it appears unlikely that such an approach will find success. The court in the *Sweeney* case, however, may not have an opportunity to address the issue because Houseparty moved to compel arbitration, and the plaintiff did not oppose.

The CCPA claim in *Hayden v. The Retail Equation*, No. 20-cv-1203 (C.D. Cal. filed 7 July 2020), presents a more nuanced variation on the *Sweeney* approach. The complaint there contends that defendant retail companies shared their customers' personal information, including purchase histories and unique identifiers, with a third party for credit risk scoring purposes. The defendants allegedly failed to disclose that they were collecting this information or that they were disclosing this information to a third party. Based on these allegations, the plaintiff seeks to bring a claim under the CCPA for violation of the statute's notice and disclosure provisions (§§ 1798.100(b), .110(c)). The complaint also claims that the defendants violated the CCPA's private right of action in section 1798.150(a) by sharing the consumers' personal information with third parties without the consumers' authorization. In other words, the plaintiff's position appears to be that the defendants' alleged failure to comply with the CCPA's notice and consent provisions means the defendant's disclosure of personal information was "unauthorized" and thus actionable under the CCPA's private right of action.

Hayden presents an important question regarding the scope of the CCPA's private right of action: whether a company-authorized disclosure to a third party can be deemed "unauthorized" for purposes of the private right of action if the consumer has not given his or her consent. There appear to be strong arguments in favor of a narrower reading because the disclosure was authorized from the perspective of the company. Moreover, even to the extent a company-authorized disclosure could be deemed "unauthorized" for purposes of the CCPA's private right of action, such a disclosure would not appear to be the result of a business's failure to maintain reasonable security practices – a necessary element of a CCPA claim. In any event, if courts were to allow claims like the one in Hayden to proceed, that could represent a dramatic expansion of the CCPA's private right of action.

Plaintiffs enforcing the CCPA indirectly

Another approach that some plaintiffs have adopted is to try to "borrow" CCPA violations as predicates for claims under the California Unfair Competition Law (UCL), which provides a cause of action for business practices that are unlawful, fraudulent, or unfair. In particular, the UCL's "unlawful" prong allows plaintiffs to borrow violations of other California laws and treat them as actionable under the UCL.

The plaintiff in *Burke v. Clearwater AI*, No. 20-cv-3104 (S.D.N.Y. filed 17 Apr. 2020), for example, seeks to recover for an alleged CCPA violation under the UCL "unlawful" prong. The complaint in that case alleges that the defendant collected and sold the plaintiff's biometric information by scraping publicly available images from the Internet to build facial recognition databases. Plaintiff contends that the defendant violated the CCPA's notice provision and thus is in violation of the UCL's "unlawful" prong. In other words, the plaintiff alleges that the defendant's collection of her biometric information was unlawful under the UCL because it did not comply with the CCPA's substantive requirements. And this CCPA violation, the plaintiff maintains, is actionable under the UCL – without reference to the CCPA's private right of action.

The difficulty facing the *Burke* plaintiff and others who would seek to adopt this approach lies in the CCPA's plain language. Section 1798.150(c) expressly states that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law." That language would appear to preclude enforcement of the CCPA through the UCL. Moreover, while the UCL's remedies typically are cumulative to those provided in other statutes, that is not true where the predicate statute "expressly provide[s]" otherwise. Cal. Bus. & Prof. Code § 17205. And as noted, the CCPA does expressly provides otherwise in section 1798.150(c). So the language of the UCL may preclude its use to expand the private right of action of the CCPA.

Relatedly, some plaintiffs have filed privacy actions based on the kinds of conduct that the CCPA regulates but under the guise of a different cause of action. For example, in *Calhoun v. Google*, No. 20-cv-5146 (N.D. Cal. filed 27 July 2020), the plaintiff claims that Google surreptitiously collected personal information, including IP addresses, browsing history, and cookie identifiers, from consumers through its Internet browser and shares that information with third parties for advertising purposes. The complaint does not assert a direct claim under the CCPA but relies on the CCPA's definition of personal information in support of a variety of privacy torts and claims under electronic surveillance laws. Another noteworthy example is *In re Google Assistant Privacy Litigation*, No. 19-cv-4286, a consolidated action in which the plaintiffs allege that the Google's AI-based smart assistant surreptitiously recorded and disclosed the private conversations of its users. Although the complaints in at least some of the underlying member cases included claims under the CCPA, those claims appear to have been removed from the current operative complaint – demonstrating the overlap between these laws and, potentially, the plaintiffs' views on the strength of those claims.

Implications of pending suits

Plaintiffs have been filing complaints with CCPA claims throughout 2020 but, to our knowledge, none has yet resulted in a decision interpreting the CCPA. But motions to dismiss are pending and fully briefed in some cases, so opinions on these issues likely will start to emerge later this year.

Even in the absence of court decisions, the complaints filed thus far are instructive in various ways. They demonstrate that plaintiffs seem to be focusing their CCPA claims on two kinds of conduct. First are data breaches, which would appear to be the intended focus of the CCPA's private right of action. Second, plaintiffs also are asserting CCPA claims based on the allegedly unauthorized collection or

disclosure of personal information across the Internet ecosystem – either by expressly relying on the private right of action or by using the other approaches described above. If allowed to proceed, these claims have the potential to expand directly or indirectly the narrow scope of the CCPA's private right of action.

AUTHORS

Simon Frankel, Cortlin Lannin and Kathryn Cahoy are Partners at Covington LLP. Rafael Reyneri is an Associate.
Emails: sfrankel@cov.com
clannin@cov.com
kcahoy@cov.com
rreyneri@cov.com

REFERENCE

1 Proposed class action that accuses children's clothing company Hanna Andersson and its online payment services provider Salesforce of failing to properly safeguard customers' sensitive data.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Switzerland's DP Act revised

David Rosenthal of Vischer reports from Zurich on new aspects of the law which is expected to enter into force in 2022.

The splitting of hairs is now over and the revision of the Swiss Data Protection Act (DP Act) has finally been completed. Following the resolution of the last differences on "profiling", the Swiss Federal Parliament passed the new law on 25 September 2020. It is expected to come into force in 2022, with some sources even suggesting summer 2022. As a next step, the supporting ordinances will now be drawn up and submitted for public consultation. How fast things now progress will of course also depend on the EU: Switzerland is still waiting for the renewal of the European Commission's adequacy decision,

Continued on p.3

Egypt's Data Protection Law enters into force in October

It is likely that the law will not be fully enforced until 2022, but businesses should start preparing now. By **Dino Wilkinson** and **Masha Ooijevaar** of Clyde & Co.

On 13 July 2020, Egypt's Government issued its long-awaited Data Protection Law[1] (Law No. 151 of 2020) (the Law), which establishes various standards and controls governing the processing and handling of personal data. The Law was published in the Official Gazette on 15 July 2020.

The Law is part of a growing trend of countries enacting comprehensive data protection laws, which

Continued on p.6

Issue 167 **OCTOBER 2020**

INTERNATIONAL report

ISSUE NO 167 OCTOBER 2020

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
David Rosenthal
Vischer, Switzerland
Dino Wilkinson and Masha Ooijevaar
Clyde & Co, United Arab Emirates
Joan Antokol
Park Legal, US
Myria Saarinen and Charlotte Guerin
Latham & Watkins, France
Yen Vu, Trung Tran and Bao Nguyen
Rouse, Vietnam
Katharine Kemp and Graham Greenleaf
UNSW, Australia
Simon Frankel, Cortlin Lannin, Kathryn Cahoy and Rafael Reyneri
Covington & Burling, US
Yimika Ketiku
Nouvelle Legal, Nigeria
Oliver Butler
University of Oxford, UK
Camilla Tabarrini
University of Venice, Italy

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

New laws adopted in Egypt and Switzerland

The influence of the EU GDPR continues to be felt far and wide. Egypt has adopted its first ever data protection law which enters into force on 16 October 2020 (p.1), and Switzerland has recently updated its 1992 data protection law, planning to retain its EU adequacy status (p.1).

The GDPR has also been a model for many African countries, several of which already have legislation in place. In this issue, we report on Nigeria's Data Protection Bill, 2020 (p.31).

How would a US federal privacy law interact with existing state level privacy laws (p.14)? In this issue we look at the private right of action under the California Consumer Privacy Act and how it might be expanded (p.29).

The *Schrems II* judgment of the Court of Justice of the European Union in July has had an impact on US business and is a major topic that will stay with us for some time, although the EU Commission is prioritising this work and is trying to find a solution for data transfers from the EU to the US (p.9). We may see revised Standard Contractual Clauses emerge before Christmas. An expensive alternative is using Binding Corporate Rules. Read on p.12 what the experience has been in 2020 with companies working with four national DPAs as lead authorities.

Professor Graham Greenleaf explores the relationship between trade agreements and new data privacy laws and Bills in Asia-Pacific countries (p.18), and together with Dr Katharine Kemp, the anti-competition developments in Australia regarding Facebook and Google (p.25).

We will return to these questions in our series of five *PL&B* webinars on German data protection legislative and judicial developments and their impact on business. The first webinar on 28 October will discuss how different laws are becoming more relevant to privacy issues, for example, in the Facebook decision of the Federal Cartel Authority (*PL&B International Report* December 2019 p.1) and the subsequent Higher Regional Court of Düsseldorf and Federal Supreme Court decisions. See www.privacylaws.com/germany for the programme and on how to register (p.8).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"I've always found *PL&B* to be a great resource for updates on privacy law issues, particularly those with a pan-EU focus. They are almost always the first to an important privacy law story, meaning that I (and all of my team and most of my clients) will quickly open a mailshot from *PL&B* to see what's going on in the world of data protection."

Matthew Holman, Principal, EMW Law LLP

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.