Online Consumer Privacy: Airlines Under Scrutiny

By Heather Zachary and Allison Trzop

In October 2012, the California attorney general's new Privacy Enforcement and Protection Unit mailed an unusual letter to Delta Air Lines. The letter warned Delta of its noncompliance with the California Online Privacy Protection Act (CalOPPA or Act).[1] At issue was CalOPPA's requirement that providers of online services make their privacy policies "reasonably accessible" to users; the State contended that the airline had failed to do just that through its "Fly Delta" mobile application. When Delta did not modify its mobile app within the 30 days specified in the Act,[2] the State filed suit despite the airline's promise to comply.[3] Delta now faces a potential civil penalty of $2,500 per download, all for a free app that was intended to provide helpful services to passengers and promote Delta's brand.

California v. Delta Air Lines, which is now weaving its way through the California courts,[4] is merely one of many recent indications that companies providing online services ignore consumer privacy laws at their peril. Even prominent companies in industries accustomed to dealing with complex and onerous regulatory schemes are being caught off guard by increasingly aggressive privacy regulators at the federal and state levels. At the same time, legislators are equipping those regulators with innovative new enforcement tools.

This article offers some lessons for airlines and others from *California v. Delta Air Lines*. Although the consequences of this litigation remain to be seen, it is already clear that companies offering mobile apps, websites, and other online services face fresh challenges—both in ensuring their continued compliance with legal obligations and in avoiding harm to their brands should consumers or the media deem their privacy protections inadequate. In short, for regulatory and reputational reasons, companies should take steps to bring their practices into compliance with the rapidly evolving state of the law.

California's Online Privacy Protections

In 2004, CalOPPA came into force in California. The Act provides that an "operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy[.]"[5] The California attorney general has stated that the definition of "online services" includes mobile apps. Thus, CalOPPA's "conspicuous posting" provision requires app providers to make their privacy policies "reasonably accessible" to users.[6] Failure to do so invites stiff penalties, up to $2,500 per violation.[7] Moreover, the State has argued that each download of an app by a Californian is a separate violation,[8] a soberingly punitive tally considering that the most popular app of 2013 was downloaded 500 million times.[9]

To promote compliance with CalOPPA, California Attorney General Kamala Harris announced in 2012 a Joint Statement of Principles, adopted by Apple, Amazon, Google, Hewlett-Packard, Research in Motion, Microsoft, and other app platform operators.[10] Shortly thereafter, Attorney General Harris issued a report providing detailed guidance to app developers and providers: *Privacy on the Go: Recommendations for the Mobile Ecosystem*.[11] Both documents were shots across the bow from California's chief law enforcement officer that she was intent on defending her state's right to legislate respecting privacy in the online ecosystem.[12]

California v. Delta Air Lines

For the past four years, Delta has offered its free Fly Delta mobile app for download in marketplaces such as Apple's iTunes Store and Google Play, as well as on its own website. As with other airline apps,[13] Fly Delta users may do such things as check in for flights, view reservations, track checked baggage, take photos, and locate airport amenities. To provide these and other services, the app collects personally identifiable information about its users, including names, telephone numbers, e-mail addresses, credit card information, frequent flyer account numbers and PIN codes, photographs, and GPS location data, the latter of which the app uses to suggest "Delta Sky Clubs Near You."

On October 26, 2012, the California attorney general sent to about 100 popular commercial app providers—including Delta and United Airlines—a notification that their apps failed to include a written privacy policy as required by CalOPPA. The letter triggered CalOPPA's 30-day grace period for operators to

Published in *The Air & Space Lawyer*, Volume 27, Number 1, 2014.

bring their apps into compliance by posting privacy policies.[14] On November 30, 2012, Delta responded to the attorney general, noting that although CalOPPA was preempted by the federal Airline Deregulation Act (ADA), Delta would voluntarily comply with the statute.[15] The attorney general did not reply. Instead, on December 6, 2012, California claimed that Fly Delta continued to violate state law and filed a complaint against Delta, the first ever CalOPPA enforcement suit for failure to publish a privacy policy.[16]

Delta fired back with a demurrer on February 11, 2013, arguing that California had failed to state a cause of action and that the attorney general had displayed a "questionable exercise of prosecutorial discretion." Delta argued, first, that the ADA completely preempted the state consumer protection enforcement action because 49 U.S.C. § 41713(b)(1) dictates that states "may not enact or enforce a law . . . related to a price, route, or service of an air carrier." Delta further maintained that, even absent ADA preemption, Fly Delta did not violate CalOPPA because the state statute's definition of "online service" neither contemplated nor included mobile apps.[17]

Following oral argument, Judge Marla J. Miller sustained Delta's demurrer. "In this instance it's services," Judge Miller said during a hearing, explaining that "I think that this case is, in effect, an attempt to apply a state law designed to prevent unfair competition, which regulates an airline's communication with consumers, and I think it's pre-empted."[18] Deputy Attorney General Adam Miller filed California's Notice of Appeal on July 8, 2013.[19]

Future of the Case

At time of writing, the *Delta* case has been fully briefed in the First Appellate District, with oral argument yet to be scheduled. It is possible that the California Supreme Court or even the U.S. Supreme Court could eventually hear the case. The U.S. Supreme Court recently took up an aviation-related preemption case, *Northwest, Inc. v. Ginsberg*, in which the Court decided unanimously that the ADA preempts a state-law claim for breach of the implied covenant of good faith and fair dealing if the claim "seeks to enlarge the contractual obligations that the parties voluntarily adopt."[20]

Preemption may carry the day in the *Delta* case as well, with the appellate courts concluding that the attorney general's CalOPPA claim relates sufficiently to "prices, routes, or services" to be barred by the ADA. Should the case follow that course, the Fly Delta precedent will become another arrow in the airlines' preemption quiver. That would be no small victory given the increasingly aggressive posture of consumer privacy regulators in the online services realm. Of course, the superior court could be overturned, leaving airlines subject to an increasingly large number of privacy laws under state police power, absent some stronger relation to "prices, routes, or services" than Delta can claim.

If the ruling is overturned on preemption grounds, the courts will then need to determine whether CalOPPA applies to mobile apps like Fly Delta. The attorney general asserts that the California legislature considered the term "online service" as referring to "any and all Internet services, other than Web sites, that made themselves available to consumers online."[21] Conversely, Delta argues that CalOPPA's definition of "online service" is instead limited to early Internet gateway technologies such as America Online and Microsoft Network (MSN).[22] Delta points to contemporaneous judicial decisions as well as technical dictionaries to support its construction. In response, the State has noted that the Federal Trade Commission (FTC) regards mobile apps as fitting within the definition of online services for purposes of a federal privacy statute.[23] And while the California attorney general has conceded that mobile apps did not exist in 2003, the State also has stressed that nothing in the statutory scheme expressly excludes applications like the Fly Delta app from CalOPPA's coverage.

Even if courts agree with the State on the applicability of CalOPPA to mobile apps, California will still need to show that Delta failed to comply with the Act's substantive requirements. For example, the State will need to demonstrate that Delta's privacy policy was not "reasonably accessible" within the meaning of CalOPPA, even though Delta provided a privacy policy on its website.[24] As discussed below, such substantive compliance issues have broad importance beyond the *Delta* case.

Managing the Legal Risks of Privacy Compliance

Regardless of the outcome of the *Delta* case, one message is apparent. In California and elsewhere, state attorneys general are staking out claims to protect consumer privacy online, including on smartphones' small screens.[25] Furthermore, they are willing to use creative, if untested, tools as they ramp up these regulatory efforts. This should bring home the need for airlines and others to take steps to proactively comply with burgeoning regulatory demands concerning mobile apps and other online services.[26] To that end, we suggest five key measures to manage legal risks relating to privacy:

1. At minimum, a company must have a privacy policy that applies to any app, website, or online service it sponsors or provides. This is an express requirement of CalOPPA and also may be required by other state or federal laws

Heather Zachary (heather.zachary@wilmerhale.com) is a partner and **Allison Trzop** (allison.trzop@wilmerhale.com) is an associate at Wilmer Cutler Pickering Hale and Dorr LLP.

depending on what information is collected and from whom. For mobile apps, the privacy policy can be adapted from a company's privacy policy for its website, subject to vetting to ensure that the policy remains technically accurate when applied to the app. For example, a company may collect photos or precise location information through its app, but not on its website. In addition, the mechanisms that consumers can use to opt out of data collection on a website (e.g., opt-out cookies) may not work on a mobile device.

2. Companies should ensure that their privacy policies are "reasonably accessible" in the case of mobile apps, or "conspicuously posted" in the case of websites. CalOPPA contains express language concerning this requirement and the attorney general has provided additional guidance. For example, website privacy policies must appear on "the homepage or first significant page after entering the Web site," or through a link or icon on the homepage that complies with specific wording, color, and typeface requirements.[27] For mobile apps, the privacy policy should be accessible both from within the app and in the app store so that consumers can view the policy before downloading the app.[28]
3. Companies should evaluate the types and sensitivity of the "personal information"[29] that they collect through an app or website and provide safeguards commensurate to the privacy risk. For example, it is prudent to obtain just-in-time consent—such as through a pop-up—before an app accesses a user's contact list or tracks the user's location. Both California and the FTC have urged this sort of "privacy by design," directing online service providers to do more than bury such disclosures in their privacy policies—rather, to obtain affirmative consent for the use of "sensitive" personal information such as geo-location, contacts, photos, calendar entries, and recordings from a device microphone.[30]
4. Companies should adopt the California attorney general's "surprise minimization" mantra as their own.[31] If a consumer may not anticipate how a company will collect, use, or share certain information, the company should make a clear and conspicuous disclosure of its practices, such as on the sign-up screen.[32] The FTC also supports this surprise minimization principle and has provided guidance on how to implement it.[33]
5. Companies should be proactive, not reactive. The FTC often seeks public comment on issues related to consumer privacy, and companies and other stakeholders should raise their voices as opportunities arise. State attorneys general also look to constituents, including companies, for input when promulgating new rules and bringing enforcement actions. And what a regulator does not know can hurt you. Finally, companies should consider working with trade associations or cooperating with similarly situated entities to engage Congress on these issues. State attorneys general can and do lobby Congress to carve out areas subject to state regulation from otherwise expansive federal preemption regimes, and they are poised to do so again in the privacy realm. Complying with federal obligations is often preferable to conforming to potentially conflicting requirements in 50 different states, some of which are sure to be more burdensome than their federal counterparts.

Conclusion

Airlines, as well as companies less shielded by robust preemption defenses, should take steps to comply with rapidly evolving privacy obligations lest they find themselves in Delta's position. Fortunately, compliance with consumer privacy regulation is usually as simple as providing transparency about a company's practices. While furnishing more detail about data handling practices may seem to run the risk of alienating some consumers, companies such as Google have asserted just the opposite when it comes to services available on mobile devices: "If we fail to offer clear, usable privacy controls, transparency in our privacy practices, and strong security, our users will simply switch to another provider."[34] Moreover, in this era of media scrutiny of online privacy, the marketplace is punishing companies that lag behind consumers' privacy expectations. Reputational damage often attends the public disclosure of data collection or use practices that customers find "creepy" or otherwise objectionable.[35]

Although some airlines and companies in other industries may view compliance with obligations like CalOPPA as burdensome, the alternative is far worse. In addition to civil penalties and enforcement actions, companies face the specter of significant harm to their brand image if they fall short in terms of privacy compliance. The issue presents a stark choice: be up front about your privacy practices in consumer disclosures or risk finding those practices splashed across the front pages in yet another news story about a transgressor in the crosshairs of privacy regulators.

Endnotes

1. Cal. Bus. & Prof. Code §§ 22575–22579.
2. *Id.* § 22575(a).
3. *See infra* notes 14, 15 (discussing the California attorney general's letter and Delta's response).
4. Superior Court of the State of California, City and County of San Francisco (CGC-12-526741); Court of Appeal, First Appellate District, Division Three (A139238).
5. Cal. Bus. & Prof. Code § 22575(a).

6. *See id.* § 22577(b)(5).

7. *Id.* § 17206(a) ("Any person who engages, has engaged, or proposes to engage in unfair competition shall be liable for a civil penalty not to exceed two thousand five hundred dollars ($2,500) for each violation.").

8. California law is ambiguous regarding how the penalty should be calculated. While the California attorney general contends that each download is a separate "violation" within the meaning of § 17206(a), the Act also could be read to mean that a failure to post a privacy policy constitutes only a single violation.

9. *Snapchat, Vine Among Top Smartphone Apps of 2013*, CBS News (Jan. 1, 2014), http://www.cbsnews.com/news/snapchat-vine-among-top-smartphone-apps-of-2013/.

10. Kamala D. Harris, Cal. Att'y Gen., Joint Statement of Principles (Feb. 22, 2012), http://oag.ca.gov/system/files/attachments/press_releases/Apps_signed_agreement_0.pdf? [hereinafter Joint Statement].

11. *See* Kamala D. Harris, Privacy on the Go: Recommendations for the Mobile Ecosystem (Jan. 2013), https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf [hereinafter Privacy on the Go].

12. Cal. Const., art. I, § 1.

13. *See generally* Susan Stellin, *Yes! Download That Airline App*, N.Y. Times, Mar. 4, 2012, at TR3, http://www.nytimes.com/2012/03/04/travel/airline-apps-that-check-you-in-map-airports-and-follow-luggage.html?_r=0.

14. *See* Complaint at exh. A, California v. Delta Air Lines, Inc., No. 526741 (Super. Ct. S.F. City & County 2013) (attaching the California AG's letter).

15. In addition to notifying Delta of the app's noncompliance, the California attorney general's letter requested additional information from Delta: "Please respond to the undersigned within 30 days of the date of this letter with the following information: a) Delta's specific plans and timeline to comply with CalOPPA; or b) why you believe this app is not covered by CalOPPA." *Id.* at exh. A, at 2. In its response, Delta contended that CalOPPA was preempted with respect to the Fly Delta app. But the airline also promised to voluntarily post a separate privacy policy on Fly Delta and elsewhere, and did so on December 7, 2012. *See* Demurrer at 6, California v. Delta Air Lines, Inc., No. 526741 (Super. Ct. S.F. City & County 2013). The attorney general did not object to Delta's proposed timeline, but instead filed suit.

16. *See* Complaint, *supra* note 14.

17. *See* Demurrer, *supra* note 15, at 2–3, 7, 11–12.

18. Karen Gullo, *Delta Wins Dismissal of California App Privacy Lawsuit*, Bloomberg News (May 9, 2013, 2:36PM), http://www.bloomberg.com/news/2013-05-09/delta-wins-dismissal-of-california-app-privacy-lawsuit.html.

19. Notice of Appeal, California v. Delta Air Lines, Inc., No. 526741 (Super. Ct. S.F. City & County 2013).

20. No. 12-462, slip op. at 1 (U.S. Apr. 2, 2014).

21. *See* Opposition to Demurrer at 12, California v. Delta Air Lines, Inc., No. 526741 (Super. Ct. S.F. City & County 2013).

22. Demurrer, *supra* note 15, at 11.

23. 15 U.S.C. §§ 6501 et seq. *See* Fed. Trade Comm'n, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804, 59,807 (Sept. 27, 2011).

24. *See* Cal. Bus. & Prof. Code § 22577(b)(5).

25. In 2012, for example, Maryland Attorney General and National Association of Attorneys General President Douglas Gansler led dozens of state attorneys general in sending a letter to Google CEO Larry Page. The letter expressed concern over Google's new unified data collection policy, which implemented changes that the AGs suggested "would be virtually impossible to avoid for the large market of users with Android-driven smartphones." *See Gansler Attacks Google's Privacy Rules*, Md. Gazette, Feb. 25, 2012, at B5. *See also* Press Release, Mass. Att'y Gen.'s Office, *AG Coakley and 35 Attorneys General Send Letter to Google Chief Regarding New Privacy Policy* (Feb. 22, 2012), http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-02-22-google-privacy-letter.html. The attention of regulators reportedly was prompted by Attorney General Gansler receiving "a deluge of calls from worried consumers." Sylvia Hsieh, *Google's Privacy Changes: Tempest in a Teapot?*, Mass. Law. Wkly. (Apr. 4, 2012), http://masslawyersweekly.com/2012/04/04/google%E2%80%99s-privacy-changes-sea-change-or-tempest-in-a-teapot/.

26. CalOPPA was recently amended, for example, to require disclosure about how website and online service operators respond to consumers' "do not track" requests. The same $2,500 penalty applies to violations.

27. Cal. Bus. & Prof. Code § 22577(b).

28. Privacy on the Go, *supra* note 11, at 5; *see also id.* at 4 ("The [Joint Statement] with the platform providers has already had an impact on privacy practices. . . . In just eight months, free apps on the Apple App Store platform with a privacy policy doubled, from 40 percent to 84 percent, and those on the Google Play platform increased from 70 percent to 76 percent.").

29. CalOPPA defines personally identifiable information broadly to include, for example: "(2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. . . . (6) Any other identifier that permits the physical or online contacting of a specific individual. (7) 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 an identifier described in this subdivision." Cal. Bus. & Prof. Code § 22577(a).

30. *See, e.g.*, FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency ii (Feb. 2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

31. Privacy on the Go, *supra* note 11, at 1, 5.

32. *Id.* at 11.

33. *See generally* Fed. Trade Comm'n, Marketing Your Mobile App: Get It Right from the Start (Sept. 2012), http://business.ftc.gov/documents/bus81-marketing-your-mobile-app; Fed. Trade Comm'n, Protecting Consumer Privacy in an

Era of Rapid Change (Mar. 2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

34. *See Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. for Privacy, Technology & the Law of the S. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Alan Davidson, Dir. of Pub. Policy, Google Inc.).

35. *See, e.g.*, Hayley Tsukayama, *Path App Under Fire for Copying Address Books*, Wash. Post (Feb. 8, 2012), http://www.washingtonpost.com/business/technology/path-app-under-fire-for-copying-address-books/2012/02/08/gIQArNFCzQ_story.html (discussing consumer backlash when media revealed that a mobile app was collecting contact information without user consent).