Courts, Regulators Should Limit Excessive Privacy Penalties

By **Doug Meal, David Cohen and Adrienne Tierney** (October 28, 2020)

Doug Meal

David Cohen

Adrienne Tierney

The potential financial consequences for running afoul of privacy and cybersecurity legal requirements are on the rise. Legislatures continue to pass privacy and cybersecurity statutes imposing onerous remedies, and regulators are taking an increasingly expansive view of their remedial authority under laws that are already on the books.

A recent Federal Trade Commission settlement highlights one of the most important examples of this trend, namely, the increasing threat of civil penalties. In U.S. v. HyperBeard Inc., the FTC imposed a $4 million penalty on a company that allegedly violated the Children's Online Privacy Protection Act by allowing third-party advertising networks to collect nonsensitive personal information from children.

The settlement drew a dissent from FTC Commissioner Noah Phillips, who argued that the penalty was excessive in light of the limited harm involved. FTC Chairman Joseph Simons, by contrast, issued a statement arguing that the penalty was appropriate in light of the need to deter behavior that Congress has outlawed.

The debate between Simons and Phillips has broad significance in the privacy and cybersecurity space. A growing number of statutes, most prominently the California Consumer Privacy Act, are imposing wide-ranging privacy or cybersecurity requirements and authorizing civil penalties for violations with little guidance on how the amounts of those penalties should be determined.

Courts and regulators should heed the advice of Phillips when applying these statutes and refrain from seeking or imposing penalties that are disproportionate to the harm caused.

U.S. v. HyperBeard

In June, the FTC filed a complaint in the Northern District of California against HyperBeard, alleging that the company violated COPPA and seeking civil penalties, a permanent injunction and equitable relief.

COPPA requires, inter alia, that online services directed to children and wishing to collect covered information about them must publicly disclose their collection practices; provide direct notice to parents; and obtain verifiable parental consent for the collection, use or disclosure of the information.[1]

According to the FTC's complaint, HyperBeard allowed third-party ad networks to collect nonsensitive information in the form of persistent identifiers from the users of its child-directed apps, and those networks in turn presented those users with behavioral advertisements based on the information collected. HyperBeard allegedly violated COPPA by failing to disclose these collection practices and obtain parental consent, thereby subjecting HyperBeard to the imposition of civil penalties under Title 15 of the U.S. Code, Section 45(m).

HyperBeard settled with the FTC concurrently with the filing of the complaint, and a judgment in the amount of $4 million was entered against the company. Because HyperBeard was unable to pay the full amount of the civil penalty, the FTC suspended that amount upon payment of $150,000.

Philips dissented, arguing that given the limited harm to consumers — HyperBeard did not collect or publicize sensitive personal information about children, and children were not contacted by strangers or otherwise put in danger — the $4 million fine was too much. He noted that "[t]he recent push to heighten financial penalties ... has been relentless, without clear direction other than to maximize the amount in every case."[2]

But, according to Phillips, civil penalties should be proportionate to the harm caused by the challenged conduct, not calculated with deterrence as the central consideration. The former approach aligns more closely with traditional principles of fairness and justice and comes with many social benefits, whereas the costs necessary to achieve complete deterrence are too great for society to bear.

In response, Simons wrote that he disagrees that civil penalties should start with harm.[3] The goal of civil penalties, in his opinion, should be to make compliance more attractive than violation. The proper starting point in this case, according to Simons, was HyperBeard's gain from behavioral advertising over the relevant time period. This, together with a number of other factors, among which was the threat posed to consumers, although not the harm actually caused, warranted the $4 million fine.

Broader Implications

The debate between Simons and Phillips has broad significance in the privacy and cybersecurity space. A growing number of statutes are imposing wide-ranging privacy or cybersecurity requirements and authorizing civil penalties for violations with little guidance on how the amounts of those penalties should be determined.

Most notably, the CCPA, whose extensive privacy requirements just became enforceable this summer, authorizes the California attorney general to seek civil penalties of up to $2,500 per violation or $7,500 per intentional violation of the CCPA after a 30-day cure period.[4]

Among the many violations subject to civil penalties are a covered business' failure to:

- Provide detailed disclosures to consumers about the collection, use, disclosure and sale of personal information, as well as consumers' rights under the CCPA;

- Provide consumers access to the underlying personal information collected about them and individualized details about their personal information in response to a verifiable request;

- Delete personal information collected from the consumer in response to a verifiable request; and

- Provide certain opt-outs to consumers regarding the collection and use of their personal information.[5]

Likewise, the New York Shield Act, which just went into effect last spring, provides for civil penalties imposed by the New York attorney general for certain failures to provide reasonable cybersecurity.[6] Covered businesses may be liable for a civil penalty of up to $5,000 dollars per violation.[7] Other examples abound.[8]

Limiting Penalties Based on Harm

Courts and regulators applying these and other penal statutes should heed Phillips' warning that the remedy should be calibrated to the harm caused. Even when a statute purports to authorize civil penalties for a privacy or cybersecurity violation without requiring the regulator to prove consumer harm, this does not mean the question of consumer harm should be irrelevant to the level of penalty imposed.

To the contrary, determining penalties with reference to harm is beneficial from a policy perspective because it forces defendants to internalize the costs their conduct has imposed on others, incentivizing them to conduct themselves in a way that produces a net benefit to society.[9]

By contrast, as Phillips noted in the 2019 FTC action U.S v. Google LLC, imposing penalties that are disproportionate to the harm caused "can deter companies from exploring innovative and consumer friendly products and services; the risk may simply be too great."[10] Such penalties can also raise due process concerns.[11] In short, limiting penalties when there has been little harm, as Phillips stated in his HyperBeard dissent, is "simply common sense."

Doug Meal is a partner and head of the cyber and privacy litigation and enforcement practice at Orrick Herrington & Sutcliffe LLP.

David Cohen is of counsel at the firm.

Adrienne Tierney is an associate at the firm.

Oladoyin Olanrewaju, a former summer associate at the firm, contributed to this article.

[1] See 15 U.S.C. § 6502(b); see also 16 C.F.R. § 312.4(b), (d); § 312.5(a)(1).

[2] Statement of Commissioner Noah Joshua Phillips, FTC v. HyperBeard, Inc., No. 1923109 (June 4, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576434/192_3109_hyperbeard_-_dissenting_statement_of_commissioner_noah_j_phillips.pdf.

[3] Statement of Chairman Joseph J. Simons, FTC v. HyperBeard, Inc., No. 1923109 (June 4, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576438/192_3109_hyperbeard_-_statement_of_chairman_simons.pdf.

[4] Cal. Civ. Code § 1798.155(b).

[5] Cal. Civ. Code §§ 1798.130, 1798.135.

[6] N.Y. Gen. Bus. Law § 899-bb.

[7] N.Y. Gen. Bus. Law §§ 899-bb(2)(d), 350-d.

[8] See, e.g., Nev. Rev. Stat. §§ 603A.300-603A.360 (empowering Nevada Attorney General to seek civil penalties for violation of privacy statute comparable to the CCPA).

[9] See, e.g., Gary S. Becker, Crime & Punishment: An Economic Approach, 76 J. POL. ECON. 169 (1968); STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 474-79 (2004); Mitchell A. Polinsky & Steven Shavell, Should Liability Be Based on the Harm to the Victim or the Gain to the Injurer?, 10 J.L. ECON. & ORG. 427 (1994); Louis Kaplow, Optimal Deterrence, Uninformed Individuals, and Acquiring Information about Whether Acts are Subject to Sanctions, 6 J.L. ECON. & ORG. 93 (1990).

[10] Separate Statement of Commissioner Noah Joshua Phillips, U.S v. Google LLC, No. 1723083 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542943/phillips_google_youtube_statement.pdf.

[11] See, e.g., State Farm Mut. Auto. Ins. Co. v. Campbell, 538 U.S. 408, 424-25 (2003) (noting that Due Process limits the degree to which awards can exceed actual damages).