# The CONSENT Act and Renewed Congressional Data Privacy Interest

April 17, 2018

As the march of highly-publicized consumer data breaches and privacy incidents continues, congressional interest in data privacy legislation is increasing. Alongside recent congressional hearings on data privacy measures, Senators Markey (D-Mass.) and Blumenthal (D-Conn.) introduced the Customer Online Notification for Stopping Edge-provider Network Transgressions Act (the "**CONSENT Act**"),[1] which if enacted would give the Federal Trade Commission (the "**FTC**") broadened regulatory and enforcement power and subject software and Internet-based businesses to heightened notice and consent requirements, together with affirmative data security and breach notification obligations. The **Davis Polk Cyber Breach Center blog** is closely following this bill, as well as other similar proposals, and will report on any significant developments.

## Purpose and Scope

The CONSENT Act's stated purpose is "to require the Federal Trade Commission to establish privacy protections for customers of online edge providers, and for other purposes."[2] To that end, it instructs the FTC to protect the privacy of consumers of "edge providers" by promulgating regulations related to the use and sharing of "sensitive customer proprietary information," maintaining "reasonable data security practices," and providing consumer notification in the event of a data breach. The bill calls for a mandatory rulemaking proceeding at the FTC within one year of its enactment, with regulations to be effective within 180 days after promulgation.[3]

As defined in the bill, "edge providers" include entities that offer services to individuals over the Internet, through software, including mobile apps, or through connected devices. While this definition would reach a large proportion of businesses offering products and services online, it does not extend to Internet service providers ("**ISPs**") (other than to the extent they engage in edge provider services or offerings).[4] "Sensitive customer proprietary information," includes financial information, health information, information pertaining to children, social security numbers, precise geolocation information, content of communications, call detail information, web browsing history and application usage history (and functional equivalents of either), and any other personally identifiable information that the FTC determines to be sensitive.[5] "Personally identifiable information" itself is defined as any information that is linked, or "reasonably may be linked," to a specific individual or device.[6] The FTC has previously suggested this final category could include "persistent identifiers such as device identifiers, MAC addresses, static IP

[1] CONSENT Act, S. 2639, 115th Cong. (2018).

[2] *See id.* preamble.

[3] *See id.* § 2(b)(2).

[4] *See id.* § 2(a)(4-5).

[5] *Id.* § 2(a)(8).

[6] *Id.* § 2(a)(9).

addresses and cookies."[7] Should the CONSENT Act become law, the FTC would likely provide additional guidance regarding the bounds of sensitive personally identifiable information during its mandatory rulemaking proceeding.

## Specific Privacy Notice and "Opt-in" Requirements

Under the bill, edge providers would be required to (i) notify customers about the collection, use, and distribution of their sensitive customer proprietary information and (ii) provide customers with information regarding the type of sensitive customer proprietary information the edge provider is collecting, specifying how and for what purposes the edge provider will be using and sharing their sensitive customer proprietary information, and identifying the types of entities with which the edge provider will be sharing such information.[8] This notice information would need to be provided when a customer first subscribes to, establishes an account for, purchases, or begins receiving an edge service, and the customer would need to be updated when the edge provider's policies relating to such information change in a "significant way."[9] Edge providers must also disclose offerings that provide customers with "discounts or other incentives in exchange for an express affirmative consent of the customer to the use and sharing of the sensitive customer proprietary information of the customer."[10]

In addition to specific notice requirements, the bill would require edge providers to obtain opt-in consent from customers to use, share, or sell their sensitive proprietary information. This opt-in consent requirement would only be satisfied through an affirmative, express consent to use, disclose or permit access to the customer's information after the customer has received "explicit notification of the request of the edge provider with respect to that information."[11] The bill would also prohibit edge providers from refusing to service customers on the basis of their choice not to consent to the use and sharing of their proprietary information for commercial purposes.[12]

Some of the notice requirements, as well as the "opt-in" consent requirement, in the CONSENT Act may be inspired by similar provisions in the European Union's General Data Protection Regulation (the "**GDPR**").[13] For example, the GDPR's notice requirements also obligate disclosure of the purposes of the data collection as well as the third-party recipients or categories of recipients with whom the data will be shared and the GDPR specifies that "pre-ticked" boxes do not constitute consent.[14]

---

[7] *See, e.g.*, Jessica Rich, Director, FTC Bureau of Consumer Protection, *Keeping Up with the Online Advertising Industry* (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[8] CONSENT Act § 2(b)(2)(B)(i).

[9] *Id.* § 2(b)(2)(B)(ii).

[10] *Id.* § 2(b)(2)(B)(v).

[11] *Id.* § 2(a)(6).

[12] *Id.* § 2(b)(2)(B)(vi) (as drafted, this provision applies to "customer proprietary information" rather than "sensitive customer proprietary information").

[13] *See* EU General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Art. 13(1)(c), (f), Recital 32.

[14] *See id*.

## Affirmative Data Security and Breach Notification Obligations

The bill would impose an affirmative data security obligation on edge providers, requiring them to develop "reasonable data security practices."[15] The FTC would likely draw on its growing body of data security guidance and enforcement actions in promulgating rules to effectuate this provision.[16] The bill also provides additional protection for de-identified information by restricting edge providers from restoring personally identifiable information that has previously de-identified.[17]

Edge providers would also be required to notify customers of security breaches where the unauthorized disclosure of sensitive user data has occurred and is reasonably likely to result in harm.[18] The bill does not provide details regarding any volume thresholds or timing guidance. Because the CONSENT Act does not include any preemption provisions, this notification requirement would likely apply in addition to other, sometimes overlapping, state and federal cybersecurity and breach notification regimes.

## Enforcement

The bill would be enforced primarily by the FTC under the FTC's authority to prohibit unfair or deceptive acts or practices ("**UDAP authority**").[19] Certain other regulators have jurisdiction with respect to specific sectors outside the FTC's jurisdiction. The FTC would also be empowered to evaluate the reasonableness of any program that relates the price of an edge service to the privacy protections afforded to customers.[20] Unlike direct enforcement of its statutory UDAP authority, where the FTC cannot impose direct fines, the FTC could impose a civil penalty of up to $40,000 per day for knowing violations of rules promulgated pursuant to the CONSENT Act.[21]

The bill also proposes that state attorneys general be granted the authority to enforce the CONSENT Act by bringing a civil action on behalf of the residents of their state against any violators to (i) enjoin that practice; (ii) enforce compliance with the CONSENT Act or regulations promulgated thereunder; (iii) obtain damages, restitution, or other compensation on behalf of residents of their state; or (iv) obtain other relief that the court considers to be appropriate.[22] The bill does not, however, include a private right of action by individuals.

## Other Privacy Bills

In addition to the CONSENT Act, Senator Blumenthal's MY DATA Act[23] and Representative Blackburn's (R-Tenn.) BROWSER Act[24] are each receiving renewed attention. Both bills were introduced in 2017, following the Congressional Review Act's repeal of Internet service provider-specific privacy rules enacted by the Federal Communications Commission. Each bill would apply to both edge providers and ISPs and

---

[15] CONSENT Act § 2(b)(2)(B)(vii)(1).

[16] *See e.g.*, Fed. Trade Comm'n v. Ruby Corp., No. 1:16-cv-02438-RBW (D.D.C. Dec. 14, 2016).

[17] See CONSENT Act § 2(b)(2)(B)(iv).

[18] *Id.* § 2(b)(2)(B)(vii)(2).

[19] *Id.* § 2(c)(2).

[20] *See id.* § 2(b)(2)(B)(v).

[21] *See* 15 U.S.C. § 45(m)(1)(A), (C) (providing that each day of a continuing failure to comply with an FTC Act UDAP rule is treated as a separate violation).

[22] *See id.* § 2(e).

[23] MY DATA Act of 2017, S. 964, 115th Cong. (2017).

[24] BROWSER Act of 2017, H.R. 2520, 115th Cong. (2017).

each bill would be enforceable by the FTC.[25] The MY DATA Act would permit the FTC to promulgate privacy and data security rules and would provide enforcement authority to state attorneys general in addition to the FTC.[26] The BROWSER Act would require edge providers and ISPs to obtain opt-in consent from users before using, disclosing, or providing access to sensitive user information and to allow users to opt-out from the use or sharing of non-sensitive user information.[27] It would not authorize FTC rulemaking and would expressly preempt state privacy laws.[28]

Senators Klobuchar (D-Minn.) and Kennedy (R-La.) have also announced their intent to introduce bipartisan privacy legislation that would, "protect the privacy of consumers' online data by improving transparency, strengthening consumers' recourse options when a breach of data occurs, and ensuring companies are compliant with privacy policies that protect consumers."[29] Additional legislative proposals may be put forward on both sides of the aisle in coming weeks.

## Conclusion

Given the heightened public attention on data privacy, we anticipate additional forthcoming bills and the possibility of regulatory action. We will monitor the CONSENT Act and other legislative proposals as they progress. For updates on further developments, please see the **Davis Polk Cyber Breach Center blog**.

---

[25] MY DATA Act § 2(d)(1); BROWSER Act § 5(b).

[26] MY DATA Act §§ 2(c), 2(e)(1).

[27] BROWSER Act §§ 3(a), 3(b).

[28] *Id.* § 7(a).

[29] News Release, Klobuchar, Kennedy to Introduce Bipartisan Legislation to Protect Privacy of Consumers' Online Data (Apr. 12, 2018), https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=E3ABA75F-685D-498F-97D2-A63EB0000E79.

---

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.


| | | |
|---|---|---|
| **Frank Azzopardi** | **+1 (212) 450-6277** | **frank.azzopardi@davispolk.com** |
| **Avi Gesser** | **+1 (212) 450-4181** | **avi.gesser@davispolk.com** |
| **Jon Leibowitz** | **+1 (202) 962-7050** | **jon.leibowitz@davispolk.com** |
| **Pritesh Shah** | **+1 (212) 450-4147** | **pritesh.shah@davispolk.com** |
| **Michelle Ontiveros Gross** | **+1 (650) 752-2073** | **michelle.gross@davispolk.com** |
| **Daniel Forester** | **+1 (212) 450-3072** | **daniel.forester@davispolk.com** |
| **Reagan Lynch** | **+1 (202) 962-7161** | **reagan.lynch@davispolk.com** |