



November 21, 2019

HOUSE AND SENATE AGREE ON ANTI-ROBOCALL BILL

On November 15, 2019, the House and Senate announced that they have come to an agreement in principle on legislation to address robocalls, titled the Pallone-Thune TRACED Act.

The press release issued by the House Committee on Energy and Commerce stated that the six House and Senate committee leaders believe that the Pallone-Thune TRACED Act can be signed into law after reaching their agreement. The press release states that the Act will require telephone carriers to verify calls and allow robocalls to be blocked in a consistent and transparent way, all at no extra charge to consumer. The press release also stated that the Act also gives the FCC and law enforcement the ability to quickly go after scammers.

In May, the Senate passed the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act and in July the House of Representatives passed the Stopping Bad Robocalls Act. The final text of the Pallone-Thune TRACED Act has not yet been made public. We will continue to track and provide updates on the legislation. Please contact us with any questions. ☐

✧ *Michael Tomkies and Lindsay Valentine.*

TOP DEMOCRATIC SENATORS RELEASE PRIVACY AND DATA PROTECTION FRAMEWORK

The ranking members of the Senate Banking Committee, Senate Commerce Committee, Senate Judiciary Committee and Senate Committee on Health, Education, Labor and Pensions released a set of principles under which they would support a federal privacy law (the "Privacy and Data Protection Framework").

The Privacy and Data Protection Framework sets forth a set of core principles that the Senators believe should be included in any comprehensive data protection legislation, including:

- Establishing Data Safeguards. A federal privacy law must establish: (i) strict limits around the use, extrapolation and retention of certain data, (ii) clear rules to limit data sharing with service providers and third parties to that which is needed to carry out the express purposes expected and authorized by consumers and (iii) greater accountability and higher standards over the way organizations retain and secure data.

- Invigorate Competition. A federal privacy law must enable consumers to: (i) have the ability to prevent their data from being commingled across separate businesses within an enterprise, and to ensure that privacy protections, including restrictions on commingling or repurposing, apply to data obtained through mergers, acquisitions or bankruptcies and (ii) take their data to the company of their preference.
- Strengthen Consumer and Civil Rights. A federal privacy law must: (i) allow consumers to control their data, including the right to know, access, delete, correct and restrict the transfer and retention of their records, (ii) require organizations that collect and store data to provide clear, concise disclosure of and justification for their privacy practices and supply consumers with meaningful options to access products or services without sacrificing their privacy and (iii) require that entities that process consumer data in automated systems must review such algorithms in order to prevent such discriminatory impact.
- Impose Real Accountability. A federal privacy law must: (i) increase Chief Executive Officer accountability, whistleblower rights and consumer redress mechanisms to ensure that corporations are held to account, (ii) allow federal enforcers to seek significant civil fines and criminal penalties, where possible, in the first instance of privacy and data security violations, (iii) provide federal enforcers with streamlined rulemaking authority to ensure that the strong legal protections imposed by the federal privacy law can evolve and adapt to new technologies and (iv) provide for state enforcement of federal protections and private rights of action.

Notably, the Privacy and Data Protection Framework does not preempt states from enacting their own privacy laws. The California Consumer Privacy Act goes into effect January 1, 2020. See our prior ALERT dated July 18, 2018.

The Privacy and Data Protection Framework could be a sign that a comprehensive federal privacy law may yet be passed by Congress. We will continue to track and provide updates on data privacy laws on both the state and federal level. Current information on state and federal privacy laws can be found in our Marketing and Privacy Digest www.dtlaw.com/Multistate-Digests/. Let us know if you have any questions. ☐

✧ *Mike Tomkies and Lindsay Valentine.*

Darrell L. Dreher
ddreher@dtlaw.com

Elizabeth L. Anstaett
eanstaett@dtlaw.com

Emily C. Cellier
ecellier@dtlaw.com

Susan L. Ostrander
sostrander@dtlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DTLAW.COM

To see previously sent ALERTS, visit our website at www.dtlaw.com

To decline future ALERTS, please contact us at ALERTS@DLT.LAW.COM. This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

Michael C. Tomkies
mtomkies@dtlaw.com

Susan M. Seaman
sseaman@dtlaw.com

Lindsay P. Valentine
lvalentine@dtlaw.com

Judith M. Scheiderer
jscheiderer@dtlaw.com

Robin R. De Leo
robin@deher-la.com



LOOKING FOR A MARKETING AND PRIVACY COMPLIANCE RESOURCE? We publish an easy-to-use reference, our **MARKETING AND PRIVACY DIGEST** that compiles the state laws governing financial privacy, fair credit reporting, telemarketing/automatic dialing and announcing devices, telephone monitoring and recording, electronic signatures and restrictions on the use of social security numbers by financial service providers. Creditors, marketers and servicers should find this resource invaluable to marketing and privacy program development and regulatory compliance. **Contact us for details.**