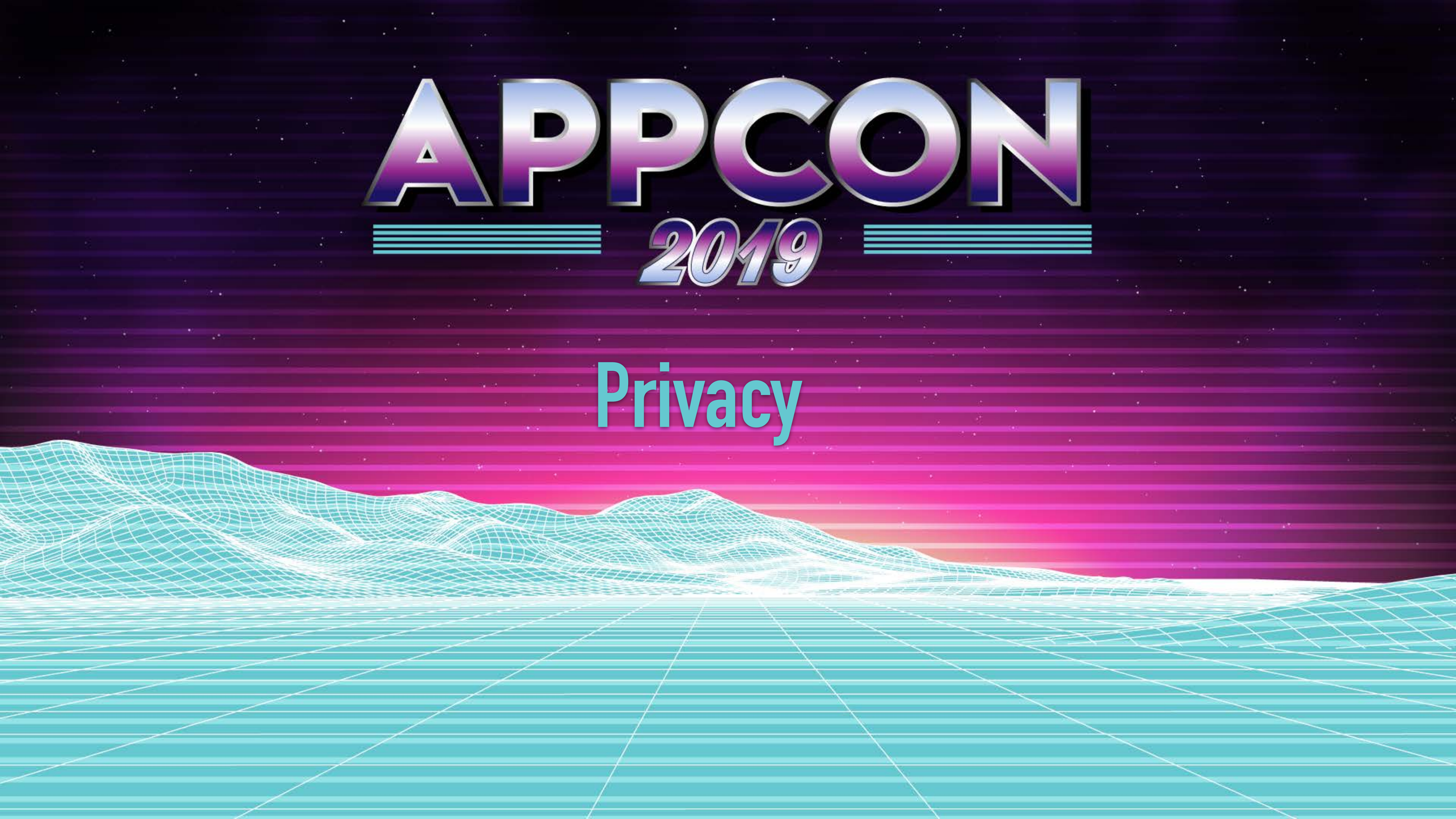
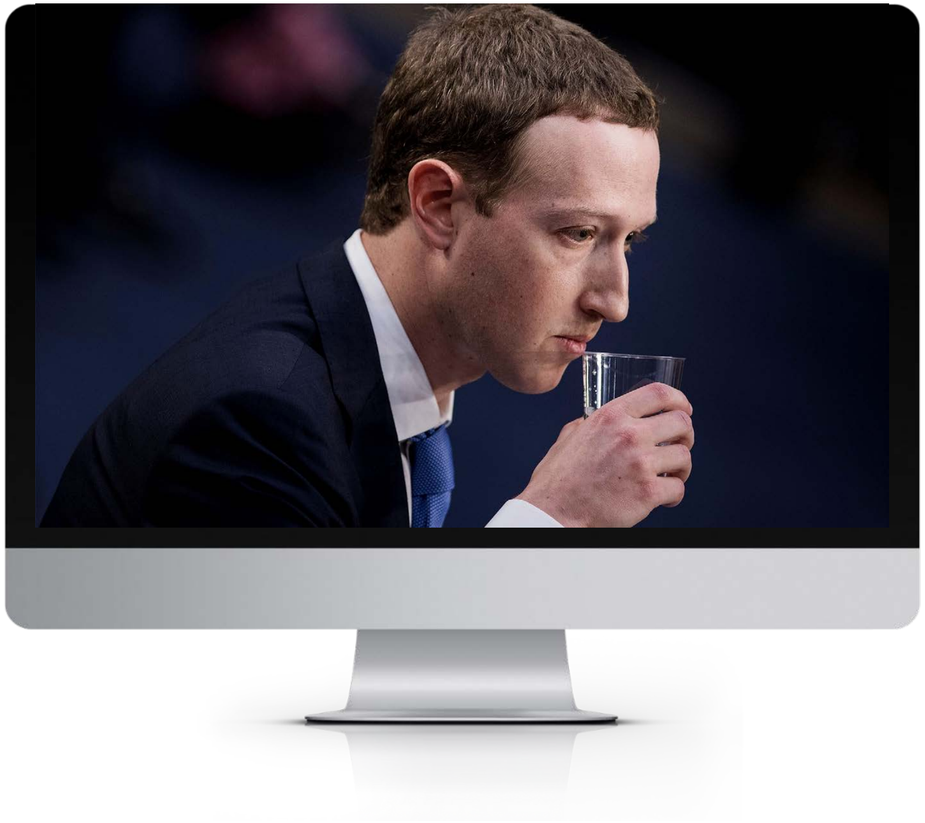

APPCON
2019
Privacy

What’s Privacy?



It’s Not Just Facebook’s Failures

01 **Facebook is the “F word” to some lawmakers and critics in DC**

02 **Facebook’s problems are mostly about advertising, or the use of data about people to target ads to them, in a poorly understood trade of personal data for free services**

03 **But privacy encompasses a much broader set of issues than the behavioral ad ecosystem**

What's Privacy?

Privacy, Not "Data Security"

01

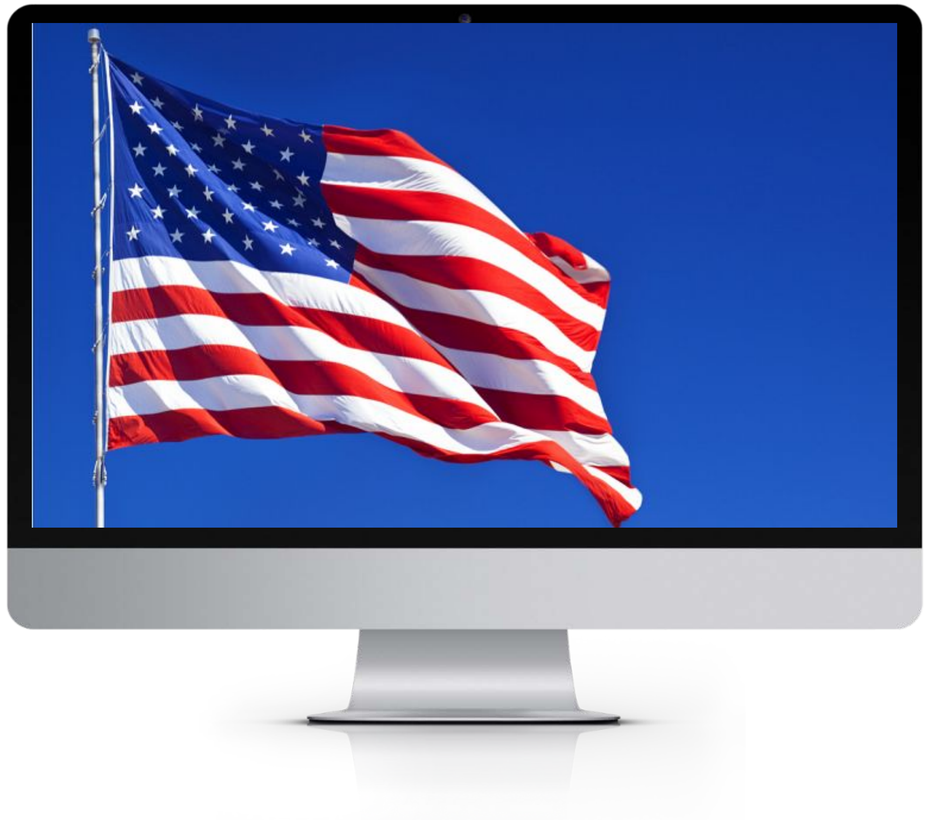
Privacy contemplates:

- Fundamentally, it's a dialogue: How companies and consumers communicate with each other about the allowable uses of consumers' data, over time and against the backdrop of changing contexts and expectations
- How people define the authorized uses of information about them and their expectations about any uses beyond explicitly authorized uses
- What companies do with information about people under the banner of consent from those people

02

Privacy is not about what a company does or does not do to protect consumer data from unauthorized access . . . that is data security

Yes, the United States has Privacy Laws



Federal Statutes and Rules

- The Federal Trade Commission (FTC) Act

01 Prohibits “unfair or deceptive acts or practices”

02 Was never intended to be a privacy statute, but the FTC has used it to stop privacy practices that are unfair or deceptive

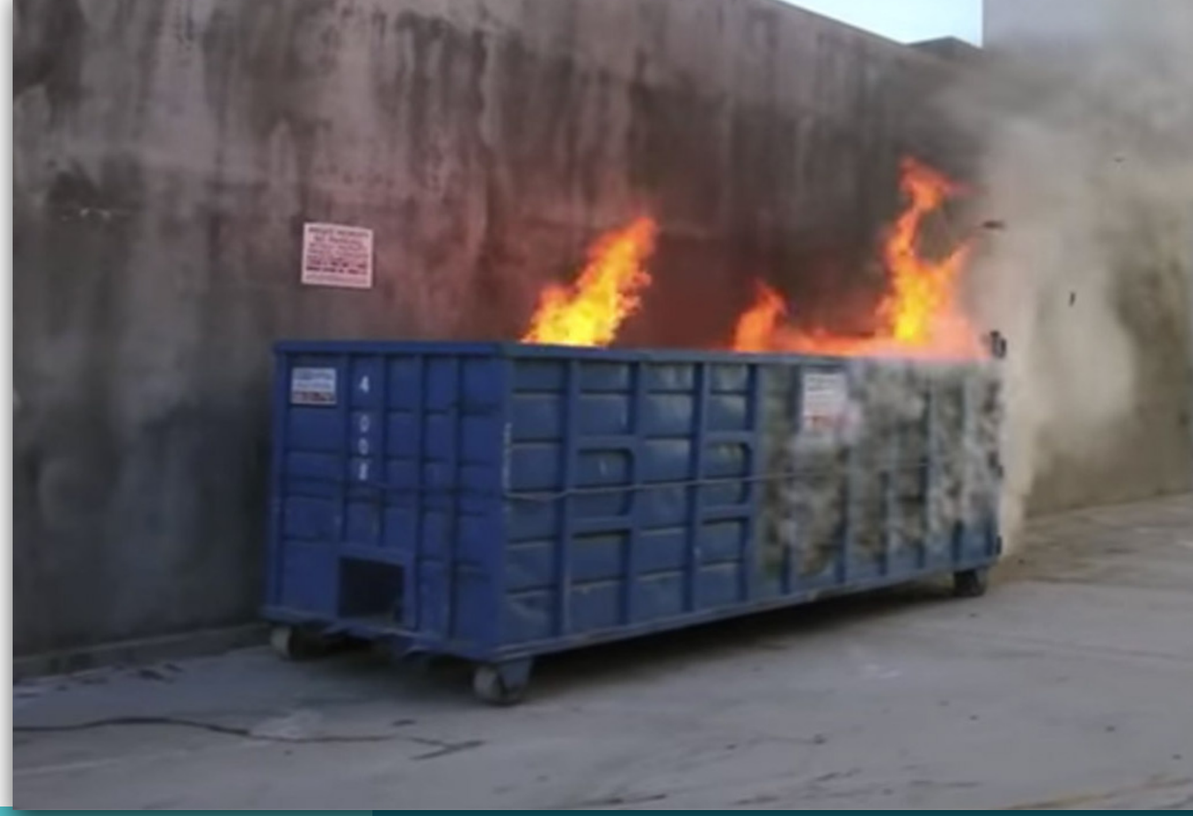
03 To help give definition to these nebulous prohibitions, the FTC periodically issues guidance and focuses on small businesses

04 Includes the Children’s Online Privacy Protection Act (COPPA), which strictly regulates the collection of data pertaining to 13-year-olds and younger

- Sector specific laws covering healthcare and financial services (but we don’t have to get into those)

The California Consumer Privacy Act (CCPA)

Goes into effect Jan. 1, 2020

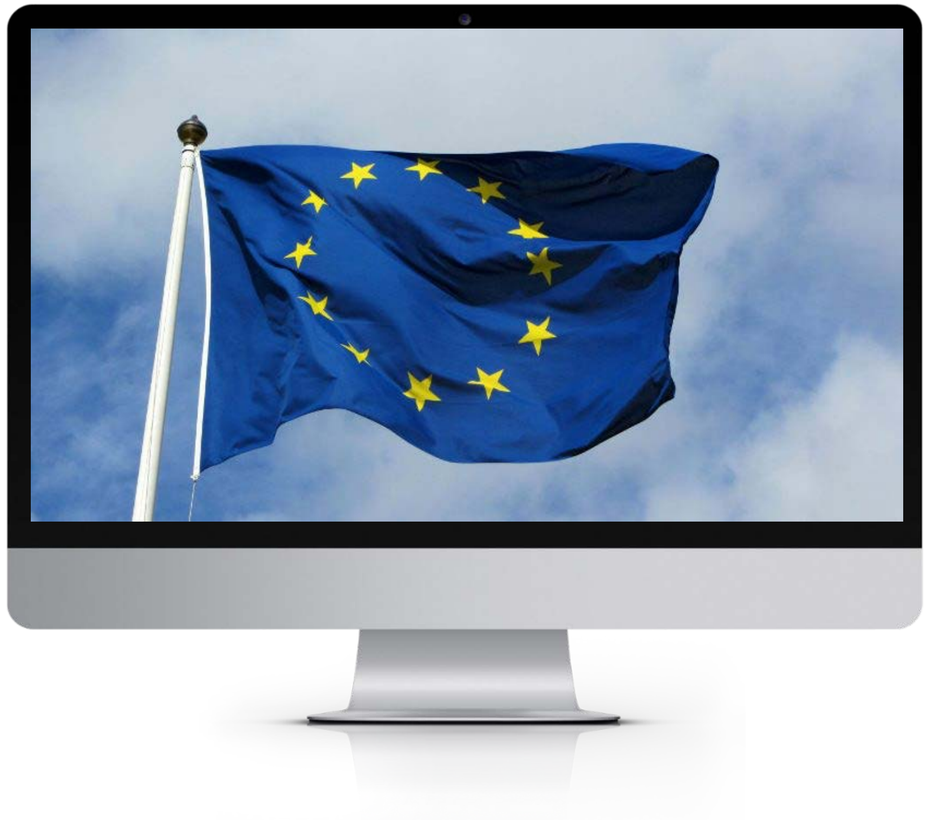


Requires companies to provide users with information about the categories of data they collect, the categories of third parties they share with, and the processing activities they engage in, upon request

Requires opt-in consent for the sharing of personal data with third parties for a “business purpose”

Allows consumers to prohibit the sale of personal data to third parties

Europeans Love Privacy



The General Data Protection Regulation (GDPR)

01 Bans processing activities involving personal data, unless one of six lawful bases for processing can be articulated and connected to the processing activities

02 Requires companies to respond to verified requests for data subjects' personal data, information about the company's processing activities and the parties with whom data is shared

03 Requires companies to respond to verified requests to delete or edit personal data, within certain limits

04 Separates "controllers" from "processors" (placing most of the compliance burden on controllers) and requires both to document and map their activities involving personal data

05 According to Google, cost the company "hundreds of person-years" to develop compliance

Are Small Companies Hopelessly Caught in the Middle?

Nope! A Federal Framework Should:

- Preempt state laws

  Can you imagine having to comply with 50 different state privacy laws, many of which have conflicting requirements? No thanks. You might get pushback on this, but there's no reason for a federal bill that just heaps on top of states. We are willing to support a strong privacy bill that would do the states proud and would enable state attorneys general to enforce.

- Allow for flexible approaches to privacy that respect changing contexts and expectations, including privacy by design

What About the Middle Ground?

Some Elements of Privacy Proposals are Workable:

• Providing consumers with reasonable control over their data, which could take the form of limited “rights” or requirements on companies to respond to consumer requests to delete, access, or edit data about them

• A flexible prohibition on activities that are net harmful (more harmful than they are good)

– For example, federal legislation could require a risk assessment, and then prohibit activities that fail the assessment

• Instead of a “small business carve-out,” scalable requirements that account for the size, scope, and complexity of an enterprise

– Instagram had 13 employees and over 30 million users when it was acquired by Facebook

– A small business distinction in the privacy context isn’t meaningful, requirements should be scalable so that smaller companies can comply and compete with larger companies

Company Killers

But Some Elements are Not Workable:

• A private right of action; this is an invitation for trial attorneys to make money off the accidental missteps of small companies

• General rulemaking; the FTC is not a rulemaking agency, it doesn’t do well with ill-defined statutory guidelines (e.g., COPPA)

• Broad definitions of personal data that include device identifiers; some privacy protection measures use automatically generated identifiers, so this requirement would defeat those privacy measures

• Requirements to re-identify de-identified or anonymized data

• A European-style “ban on processing” except for limited lawful bases

What Was That Again?

Preemption.

If Congress drafts a bill, it should establish a single, national set of rules to avoid conflicting state regimes that would ultimately be a compliance nightmare without improving consumer privacy

But allowing state attorneys general to enforce the federal laws is okay

Reasonable Control.

A federal law should require companies to communicate their data processing activities to users and require them to respond to reasonable and verifiable requests for access, deletion, and editing of data about them

Privacy by Design.

Requirements should enable privacy by design instead of killing it with compliance—one way of doing this is not to overly restrict processing activities but require risk assessments

Scalable Requirements.

Requirements should be scalable depending on the size, scope, and complexity of an enterprise (these caveats are in the FTC's current enforcement authority)