WORLD **PRIVACY** FORUM

Media Contact:
Pam Dixon
World Privacy Forum
760-712-4281
www.worldprivacyforum.org

October 10, 2018

WORLD PRIVACY FORUM STATEMENT ON FEDERAL PRIVACY LEGISLATION

Portland, Oregon: Consumer data privacy comprises the core of World Privacy Forum's mission and purpose. A meaningful part of our work and research has focused on data brokers and secondary uses of consumer data. The debate over what the contours of federal privacy regulation should look like must be inclusive of the lynchpin issues of secondary and tertiary uses of consumer data.

WPF Executive Director Pam Dixon says: "Through our longstanding work regarding data brokers and related harms to consumers, it is abundantly clear that if Congress enacts privacy legislation that fails to effectively regulate data brokers and stop the consumer harms they directly cause, any legislation enacted will be a failure."

Privacy legislation in the U.S. has a long and storied history. However in all of the rich legacy of privacy law there exists a gap that is still unresolved: there are not controls over most secondary uses of data and tertiary sales or uses of consumer data. Nowhere has this deficit been more problematic than in the data broker industry. The World Privacy Forum has spent years researching and documenting data broker practices.

Our research has found:

- Data brokers sell, trade, and share highly sensitive and identifiable information about consumers - usually without any knowledge on the part of consumers about these activities. WPF has meaningfully and repeatedly documented that data brokers sell information about consumers who have bought a particular item, take certain medications, read certain books, or engage in certain activities. Thousands of data broker lists exist, with millions of consumers identified in the lists by name.

- The data broker industry has evolved to also focus on detailed consumer data analysis that results in predictive profiles of consumers, often with a score attached. WPF calls this "consumer scoring," and we documented these practices extensively in our report, *The Scoring of America*.

- Consumer scoring covers everything from consumer loyalty to employability to personality scores to medical risk scores, and more. These analytical scores become a kind of shorthand to describe consumers and can influence meaningful marketplace opportunities in consumers' lives. Again, without consumers' knowledge or control.

- Data brokers, data compilers, and large technology platforms do not have absolute control of tertiary uses of data, including malicious uses. Consumers in particular do not have enough controls over their data. Real consumer harms can result from secondary and tertiary uses, and the harms can continue forward for years in some cases. When consumer data escapes into third party hands, there are almost no existing controls for fully recapturing the escaped data or fully understanding everywhere the data might have gone. This is illustrated by the Facebook Cambridge Analytica scandal, by the Equifax data breach, and most recently, by the Google + data breach.

Solving the problem of applying meaningful controls of secondary and tertiary sales and uses of consumer data must be at the core of what gets resolved in any federal privacy legislation. If federal privacy legislation does not address this set of core issues, then the secondary uses gap will continue unabated, and no real privacy can be had as long as this gap exists. This gap can be narrowed by meaningful work to provide:

- Consumer controls of certain data flows and data uses, including long-term controls,
- Creating transparency, choice, and meaningful rights around consumer scoring,
- Creating technological, procedural, and policy controls over secondary and tertiary data uses. This can range from data tracking techniques to standards for de-identification to technological measures that audit data for inappropriate/appropriate uses over its lifetime.

No one expects perfect solutions. But if solutions do not address the lynchpin of the consumer privacy data challenges, then we will not accomplish what we need to.