DATA FLOWS, TECHNOLOGY, & THE NEED FOR NATIONAL PRIVACY LEGISLATION

BREACHES DRIVING PRIVACY LEGISLATION

Responding to recent widely-covered data breaches and privacy violations, state lawmakers have passed or are proposing privacy legislation with dramatic differences—including some draconian data security enforcement provisions. A patchwork of rules is emerging, causing business uncertainty and consumer confusion.

CONGRESS MUST ACT

Congress must act to pass a privacy law that eliminates a confusing patchwork of state laws while protecting consumers and promoting innovation. Sensible federal legislation will reduce consumer burdens and protect competitiveness and innovation, hallmarks of the American economy. Failure to act soon jeopardizes the American economy as the privacy patchwork emerges.

TECH AND DATA VITAL TO US ECONOMY

The ability to innovate with data has helped American firms achieve global dominance in tech, the industry of the era, and has promoted growth and prosperity for a generation. A patchwork of state privacy laws or a badly-crafted federal privacy law with excessive data security provisions threatens the long-term vitality of the tech sector and the US economy.

MISPERCEPTIONS ABOUT RISKS FROM DATA BREACHES

There is a "Jaws effect"— reluctance to swim in ocean owing to fear of shark attack—associated with data breaches. Widely-held fears of data breaches leading to consumer harm are unsupported by decades of evidence. The public attention to breaches, using a common narrative focusing upon major breaches, sustains and feeds rampant fears about risks to consumers from breaches despite no supporting evidence. Breach misperceptions are eroding consumer trust in tech and influencing lawmakers.

MAJOR STUDY OF BREACHES AND CONSUMER IMPACTS

This study is the most comprehensive study of the consumer impacts from data breaches to date. It involves data on three levels of analysis—macro, micro, and case studies—a rich array of variables to test possible impacts going back fifteen years.

WEAK LINK BETWEEN BREACHES AND ID THEFT

For the last 14 years, data breaches have been increasing, while the rate of ID theft remained relatively constant, fluctuating between 4.35% and 6.63%. Therefore, the incidences of data breaches and volume of records breached do not predict incidences of ID theft.

BREACHES GROW WHILE ID THEFT/FRAUD LOSSES DECLINE

Over the past decade, the number of data breaches and records stolen has increased, while fraud losses declined from a 2005 high of $35 billion to under $15 billion in 2018. There is no strong positive relationship between data breaches and ID theft and fraud losses.

NO EVIDENCE THAT BREACHES BROADLY HARMING CONSUMERS

Data on 27 million persons enrolled in credit monitoring at a national credit bureau, including roughly 5 million victims of data breaches, did not show breaches cause direct consumer harm. Credit scores increased for breached consumers and breach victims had less dark web data leakage than the comparison samples. Rates of credit activity and credit locks, possibly indicating ID theft, for the breach victims were lower than for the comparison samples.

BREACHES NOT A MAJOR DRIVER OF ID THEFT

PERC analyzed 24 notable reported data breaches in the US over the past 15 years and found the highest ID theft rate linked to a data breach to be 2.5%, from a particular data breach in 2013. This is less than half the average identity theft rate of the general population, which was 5.32% between 2005 and 2018.