UNCAPPED POTENTIAL
CABLE ACADEMY 2017
April 19 & 20
Kalahari Resorts in the Poconos

RESERVE YOUR KALAHARI POCONOS RESORT ROOM AT THE CABLE ACADEMY GROUP RATE OF $149!

Online booking is closed. Secure your discount by calling 877-525-2427 and use Group Booking ID# 1597.

CONFIRM YOUR **SPONSORSHIP**, **REGISTRATION** AND **EXHIBIT** *(exhibit covers your Cable Academy registration!)*

BCAP 60th Anniversary

NewsClips

April 3, 2017

York Daily Record
Pa. Republicans help overturn online privacy rules

Politico
How a telecom-tech alliance wiped out FCC's privacy rules

Bloomberg
Internet privacy furor previews coming war over net neutrality

Fortune
Trump's Tech Agenda Is Winning

Motley Fool
The Biggest Risk Facing Frontier Communications

Allentown Morning Call
Pro-Trump nonprofit launches TV ads in Pa.

Philadelphia Inquirer
Will McCord's testimony sink other corruption cases?

pennlive.com

Legislation approved by the Minnesota House and Senate this week would prevent ISPs from collecting personal information without written approval from customers. The quick action came in response to the US House and Senate voting to eliminate nationwide rules that would have forced ISPs to get consent from Americans before using or selling **Web browsing history** and app usage history for advertising purposes.

When the Minnesota Senate on Wednesday discussed a budget bill, it added an **amendment** that says ISPs may not "collect personal information from a customer resulting from the customer's use of the telecommunications or Internet service provider without express written approval from the customer." The amendment would also prohibit ISPs from refusing to provide services to customers who do not approve collection of personal information.

The Minnesota House added a **similar amendment** to its own budget bill on Tuesday, according to a ***Pioneer Press* article**. Democratic state Senator Ron Latz proposed the amendment in the Senate. While the amendment doesn't specifically mention browsing history, the text may be broad enough to cover such collection, and a **statement from Latz** said his intent is to prevent ISPs from selling "browsing history, health data, financial information, online purchase data, app usage and geo-location."

Editorial: Tired of the corruption in Pa. politics? It's up to you to make the change	"This amendment is about standing up and saying that our online privacy rights are critically important," Latz said. "The amendment states that Minnesotans shall not have their personal information from their use of Internet or telecommunications services collected by providers *without* their express written approval. It won't circumvent the federal government, but it will give Minnesotans a legal recourse to protect their privacy." The Senate and House versions of the budget must be reconciled into a compromise version before final passage, the *Pioneer Press* noted. Republicans have a one-vote majority in the Minnesota Senate, but one Republican sided with Democrats in order to get the amendment into the Senate's final bill. "We should be outraged at the invasion that's being allowed on our most intimate means of communication," said Republican Sen. Warren Limmer, according to the *Pioneer Press*. "This is an amendment that so urgently needs to be addressed." Republicans have a 77-57 advantage in the Minnesota House, while Minnesota Governor Mark Dayton is a Democrat. President Trump is expected to sign off on **Congress' decision** to kill the Federal Communications Commission privacy rules. While there wouldn't be any rules for ISPs at the national level, states could try to implement some form of the FCC rules for their own residents. ISPs might conceivably change their practices nationwide if enough states do so, or customers in some states could have fewer privacy protections than customers in other states. "As on climate change, immigration and a host of other issues, some state legislatures may prove to be a counterweight to Washington by enacting new regulations to increase consumers' privacy rights, a *New York Times* **article** said this week. The *Times* article mentioned laws in California, Connecticut, Nebraska, and West Virginia and proposals for new laws in Illinois, Hawaii, and Missouri, but none of these laws and proposals was specifically targeted at ISPs. – ***Ars Technica*** _____ Google and the Justice Department are clashing in courtrooms across the country over the government's power to compel the company to turn over emails and other personal data sought in criminal probes. The tensions deepened following **a landmark court ruling** last year declaring private online communications stored overseas off limits to prosecutors—even if there's probable cause to suspect the data contains evidence of a crime. Law-enforcement authorities send Google thousands of requests a year for user data in probes ranging from investigations of human trafficking and child pornography to terrorism and white-collar cases. Google's "legal investigations support" team is responsible for finding and disclosing matching records, often taking weeks to complete a single request, according to the company. Until a few months ago, Google turned over data demanded in warrants regardless of where content was stored to comply with a 1986 federal statute that created safeguards over electronic communications and established disclosure procedures. Google, a unit of Alphabet Inc., changed its policy last year when a New York federal appeals court became the highest judicial body to rule that data on foreign servers is beyond the reach of warrants. That case was brought by Microsoft Corp., which sought to quash a search warrant in a drug-trafficking probe seeking data in Ireland. Within hours after the ruling by the Second U.S. Circuit Court of Appeals, Google halted the processing of all search warrants. Coordinating with hundreds of employees, the company quickly developed tools to identify and filter out data stored overseas, Google said in court documents. Weeks later in August, Google lifted the moratorium. But it no longer discloses emails, videos, photos and other data that it believes are stored overseas. The company has the support of other tech companies, including Microsoft, Yahoo Inc., Apple Inc. and Amazon.com Inc. Google's tighter lid on data has angered federal prosecutors, who say the tech firm is impeding investigations. "When any provider refuses to follow court orders, investigations are jeopardized, and sometimes end unsuccessfully," said Justice Department spokesman Peter Carr. "The Justice Department is holding Google to its legal obligation." In at least one case, involving a warrant in a wire-fraud probe, the government has asked a court to hold Google in contempt. In January, prosecutors told a U.S. magistrate judge in San Francisco that the company had wrongly withheld "volumes of data" and has "frustrated ongoing efforts to locate the perpetrators." Google, in turn, asked the judge to quash the warrant and possibly "investigate the government's conduct" in the dispute, saying it's sought "diligently and in good faith" to comply with its obligations. The law in question is the Stored Communications Act, a pre-internet age statute authorizing the government to compel the disclosure of electronic records with a judge-approved

warrant based on probable cause. It's a fight Google says it tried to avoid. Court papers describe failed attempts at "constructive dialogue" with the Justice Department.

In the wire-fraud case in San Francisco, Google said in court papers that its data-location tools enabled it to disclose more emails it could now confirm were domestically stored. Prosecutors say Google is still holding back email attachments, calendar data and photos that could be important evidence. There hasn't been any ruling in this case yet.

The fight in some ways **echoes Apple's confrontation** with the Justice Department last year over whether the company could be forced to unlock a terrorist's iPhone. The standoff ended after the government said it bought a phone-hacking tool to crack the device without Apple's help.

While both disputes are examples of a major tech company throwing down the gauntlet to prosecutors, the privacy concerns in Google's legal fight are more opaque, according to American University law professor Jennifer Daskal, who specializes in national security law. Google has likened the government's demands to requiring a U.S.-based hotel chain to hand over a customer's suitcase located in a foreign hotel.

But Google's customers don't know where their data is stored, as a federal magistrate judge in Philadelphia observed. Data is dispersed across data centers. An email with an attachment can be located in the country and abroad simultaneously. That's because, as a Google told judges, a file can be split into "smaller chunks" and stored in separate servers. Lawyers for Google and other tech companies say it's not just customer privacy at issue. Turning over foreign data risks an intrusion upon foreign sovereignty that could provoke countermeasures, they have argued.

In a brief supporting Google's position, Microsoft and Apple said the government's position "invites foreign nations to reciprocate by likewise demanding that local offices of U.S. technology companies turn over U.S. citizens' private communications stored on U.S. soil." The Justice Department, for its part, says Congress never intended to create such an investigative impediment. "Because Google's data moves across its global network automatically and does not persist in any one geographic location," the government told a Wisconsin federal court in March, "the Microsoft decision renders such data inaccessible."

Since the Second Circuit's Microsoft decision, at least two lower federal courts in other jurisdictions—Philadelphia and Milwaukee—have disagreed with the holding. Judges there said requiring Google to produce data stored abroad was lawful because the collecting and searching of the records occurred in the U.S. Google has urged those judges to reconsider. Google says it agrees with the Second Circuit's interpretation of the law. But as a matter of policy, it doesn't think the legal standard should be based on where data is stored, but rather on user location. "Only Congress can create a new and lasting framework for this process." said a Google spokesman. "Absent congressional involvement...I see this issue percolating up to the Supreme Court," said Ms. Daskal. – ***Wall Street Journal***