
FEDERAL TRADE COMMISSION
UNITED STATES OF AMERICA
MCMXV

its net neutrality rules, it chose to reclassify "Broadband Internet Access Service", or "BIAS" as a Title II common carrier service.[2] (I'll talk a lot more about BIAS later.) This affected the FTC's oversight of BIAS providers. Although the FTC has general jurisdiction, there are a few carve outs, including common carriers acting as common carriers.[3] Thus, the FCC's reclassification affected the FTC's long-standing authority to protect consumers' privacy in their interactions with their broadband internet service providers.

Subsequently, the FCC decided to step into the consumer protection gap that it created. In fact, tomorrow the FCC will vote on a proposal to set privacy rules for BIAS providers.[4] We haven't yet seen the full Notice of Proposed Rulemaking, but FCC Chairman Tom Wheeler did release a fact sheet summarizing the proposal at a very high-level.[5] Therefore,

tend to be biased in at least three ways. Let me describe each of these three potential biases and how regulators can avoid such biases.

First, privacy rules ought to avoid a bias toward the privacy preferences of the few. We know that consumer privacy preferences differ greatly depending on the type of data and its use. On one hand, consumer preferences are fairly uniform with regard to certain uses of sensitive data. For example, the overwhelming majority of consumers object to unauthorized third parties using their financial data to debit their bank accounts or to open credit cards in their names. On the other hand, we know from experience as well as academic research – including a recent Pew study – that for other kinds of data and uses, people have widely varying

For types of data and uses where consumers have widely varying privacy preferences – such as advertising – we use our deception authority to promote marketplace competition to satisfy this wide range of consumer preferences. A functioning market requires companies to keep their promises. Under our deception authority, then, we bring a case when a company makes privacy promises to consumers that materially affect consumers' actions, but the company does not keep those promises. This deception-based approach encourages companies to develop privacy practices that accommodate widely varying consumer privacy preferences.

Under our unfairness authority, however, we have found certain privacy practices to be unfair, even if a company has made no promises to a consumer. Specifically, our unfairness authority prohibits practices that cause substantial harm that is unavoidable by consumers and which is not outweighed by benefits to consumers or competition.[10] Practices that the FTC has found unfair consistently match practices that consumers generally reject. For example, we brought an unfairness case against a data broker that sold sensitive financial information to individuals whom the data broker knew or should have known were identity thieves.[11] Other privacy violations with substantial harm involve accessing medical information, real time location data, and information about children without consumers' express consent.

Thus, unfairness establishes a baseline prohibition on practices that the overwhelming majority of consumers would never knowingly approve. Above that baseline, consumers are free to find providers that match their preferences, and our deception authority governs those arrangements.

---

[10] *See* 15 U.S.C. § 45(a)(1) (2012) (providing that"[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful").

[11] Fed. Trade Comm'n, In the Matter of Sequoia One, LLC, https://www ftch <<>>BDC ing th2.4(v47 45/ei)-5.1n(w)-1.2ar

In establishing the proper baseline of prohibited practices, regulators must avoid bias. If regulators set the baseline too low, it would not stop harmful practices that most consumers oppose. Too high, and it would prohibit services many consumers would prefer. Indeed, too-high a privacy baseline –

"personal information," "data," and "personal data." We will have to see what the NPRM proposes on this.

The third, catch-all category in the FCC's proposal includes any uses of data not in the other two categories. The proposal would require ISPs to get consumers to opt in for any use in this category. Thus, the FCC's proposal appears to prohibit any data use *except* for the few uses covered by the previous two prongs, absent express consumer consent. This opt in requirement appears to go beyond the obligations faced by other companies in the internet ecosystem.

Some privacy advocates, apparently frustrated with the privacy practices offered in today's marketplace, applaud the FCC's proposed precautionary approach to data use.

to overestimate potential future harm.[15] Regulators, too, face this same problem.[16] Regulation, therefore, often reflects the status quo, and, in extreme cases, unintentionally precludes future beneficial developments. In the area of privacy, notice and choice frameworks can be biased against future uses of data. For example, an effective and transparent opt-in framework typically requires that companies know at the time of collection how they will use the collected information. Yet data, including non-sensitive data, often yields significant consumer benefits from uses that could not be known at the time of collection. Mandating opt in consent for uses of certain types of sensitive data such as credit card numbers or SSNs may reflect consumer preferences, and I have supported such requirements in my time at the FTC. But if such mandates are applied to non-sensitive data, the inherent bias of such frameworks against future uses likely will reduce future benefits.

are the requirements that other internet companies face. Which brings me to my third concern about bias.

Privacy regulation ought to treat like-situated companies alike. Economists (and common sense) tell us that if different sets of rules govern competitors, companies subject to the more onerous or unpredictable regime are disadvantaged compared to those outside that regime. This may damage competition or artificially distort the market as companies seek to avoid the more onerous regime.

The FCC proposal would regulate how broadband ISPs may use subscriber data. It appears to impose stricter rules on ISPs than those under which edge providers, such as Google, Yahoo, or Facebook, for example, operate. Some have argued that it makes sense for the rules to differ. They claim that ISPs are uniquely situated to collect consumer information because all of a consumers' communications travels over the ISP's network. If this was ever true, it is not true today. As Peter Swire's recent working paper concludes, ISPs have neither a comprehensive nor unique window into consumer data.[18] Consumers multi-home, using multiple ISPs throughout the day. They connect to the internet through their home broadband connection, their mobile device connection, their employer's network, or their local coffee shop's Wi-Fi. Each of these

network comes from a piece of hardware or software that has perhaps an equally comprehensive view of the consumer's activities. And as internet services increasingly encrypt their traffic, the data which ISPs can access diminishes. In short, I remain unconvinced that ISPs have access to types or volumes of consumer data so unique that it justifies a special set of particularly strict rules.

Privacy advocates have been seeking for years to impose stricter privacy obligations across the Internet ecosystem, including on edge providers and ad networks, the Googles and Facebooks of the worss(v /P <Span>>BDC -0.04 T6c -0.002 (hor)39 0 811.04 30811.01)]TJ 010(rc(r)-1(c c(r)-

consumers' choice will be limited and consumers will be worse off. If privacy rules prevent beneficial future uses of data, innovation will suffer. And if privacy rules hamper one group of competitors to the benefit of another group, competition will be reduced.

When the FCC releases its privacy NPRM, I hope it will analyze how it can accommodate varying consumer preferences regarding different types of data, permit future beneficial uses of data, and avoid the negative competitive effects of disparate regulation.

Thank you again for having me, and I'd be glad to take any questions you might have.