AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive

By

Staff in the Office of Technology and The Division of Privacy and Identity Protection
February 13, 2024

You may have heard that "data is the new oil"—in other words, data is the critical raw material that drives innovation in tech and business, and like oil, it must be collected at a massive scale and then refined in order to be useful. And there is perhaps no data refinery as large-capacity and as data-hungry as AI. Companies developing AI products, as we have noted, possess a continuous appetite for more and newer data, and they may find that the readiest source of crude data are their own userbases. But many of these companies also have privacy and data security policies in place to protect users' information. These companies now face a potential conflict of interest: they have powerful business incentives to turn the abundant flow of user data into more fuel for their AI products, but they also have existing commitments to protect their users' privacy.

Companies might be tempted to resolve this conflict by simply changing the terms of their privacy policy so that they are no longer restricted in the ways they can use their customers' data. And to avoid backlash from users who are concerned about their privacy, companies may try to make these changes surreptitiously. But market participants should be on notice that any firm that reneges on its user privacy commitments risks running afoul of the law.

It may be unfair or deceptive for a company to adopt more permissive data practices—for example, to start sharing consumers' data with third parties or using that data for AI training—and to only inform consumers of this change through a surreptitious, retroactive amendment to its terms of service or privacy policy.

When it comes to unlawful conduct, the FTC has a long history of challenging deceptive and unfair practices in connection to a company's privacy policy that affect the promises the company made to consumers. Nearly two decades ago, the FTC charged Gateway Learning Corporation, known for its "Hooked on Phonics" products, with violating the FTC Act after it changed its privacy policy to allow it to share consumer data with third parties without notifying consumers or getting their consent.

Similarly, this past summer, the FTC alleged that a genetic testing company violated the law when the company changed its privacy policy to retroactively expand the kinds of third parties with which it could share consumers' personal data. The company did that without notifying consumers who had previously shared personal data or obtaining their consent, said the FTC.

Even though the technological landscape has changed between 2004 and today, particularly with the advent of consumer-facing AI products, the facts remain the same: A business that collects user data based on one set of privacy commitments cannot then unilaterally renege on those commitments after collecting users' data. Especially given that certain features of digital markets can make it more difficult for users to easily switch between services, users may lack recourse once a firm has used attractive privacy commitments to lure them to the product only to turn around and then back out of those commitments.

The FTC will continue to bring actions against companies that engage in unfair or deceptive practices—including those that try to switch up the "rules of the game" on consumers by surreptitiously re-writing their privacy policies or terms of service to allow themselves free rein to use consumer data for product development. Ultimately, there's nothing intelligent about obtaining artificial consent.