abuses.[4] Yet the growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used[5]—means that potentially unlawful practices may be prevalent, with case-by-case enforcement failing to adequately deter lawbreaking or remedy the resulting harms.

Indeed, a significant majority of Americans today feel that they have scant control over the data collected on them and believe the risks of data collection by commercial entities outweigh the benefits.[6] Evidence also suggests that the current configuration of commercial data practices do not actually reveal how much users value privacy or security.[7] For one, the use of dark patterns and other conduct that seeks to manipulate users underscores the limits of treating present market outcomes as reflecting what users desire or value.[8] More fundamentally, users often seem to lack a real set of alternatives and cannot reasonably forego using technologies that are increasingly critical for navigating modern life4 0 0 8.04 385.08 575.4 Tma(.-4 (r)-1 (0 (nt1g80f Tma(.-4 (r) p

more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.[13] Are there contexts in which our unfairness authority reaches a greater set of substantive limits on data collection?[14] When might bans and prohibitions on certain data practices be most appropriate?[15]

- Administrability: Information asymmetries between enforcers and market participants can be especially stark in the digital economy. How can we best ensure that any rules that we pursue can be easily and efficiently administered and that these rules do not rest on determinations that we are not well positioned to make or commitments that we are not well positioned to police? How have jurisdictions successfully managed to police obligations such as "data minimization"?[16]

- Business models and incentives: How should we approach business models that are premised on or incentivize persistent tracking and surveillance, especially for products or services that consumers may not be able to reasonably avoid?[17]

- Discrimination based on protected categories: Autol1-2 (ur)tionsng an45.76 576(l)--2 (e)4 (t)-2 0 0 iice l(

- Workplace surveillance: Reports suggest that extensive tracking, collection, and analysis of consumer data in the workplace has expanded exponentially.[20] Are there par(t)-2 (1i4uB4.64 0 7(h)/l)