

# Data privacy: what does the future hold?



## **Written by**

[Tarun Ramadorai](#)

## **Published**

13 November 2019

## **Category**

[Technology](#)

## **Key topics**

[Consumer Behaviour](#), [Data Privacy](#), [Technology](#)

## **Data privacy is a major concern for businesses, governments and consumers alike - and with the future of this thorny issue so uncertain, analysis is crucial**

Since the [Cambridge Analytica data breach](#) made headlines, data privacy has leapt to the top of the agenda for an internet-focused world facing an uncertain future. The leak saw tens of millions of Facebook profiles harvested, with the data used to predict voter behaviour and target political campaign content in the US.

Combined with the introduction of the General Data Protection Regulation (GDPR) in Europe shortly after, the event caused a rapid shift in how much consumers know about what online data is used for, and the degree to which they value their data privacy.

### **Private lives**

The issue now facing the US and the wider world is how to manage data privacy in future, with a mind to preventing data being used in ways consumers object to. Regulation is one option in this respect. The GDPR, for example, has been billed as "the most important change in data privacy regulation in 20 years", but it remains to be seen whether it is an effective way to prevent such issues as the Cambridge Analytica leak.

For one thing, consumers – whether online or offline – behave paradoxically; asked if they care about data privacy the vast majority are clear that they do, but given the chance to make decisions (e.g. about which companies they use and what websites they visit) on the basis of data usage, [many take no action](#).

Consumers often call for increased privacy protection, but then quickly suffer "consent fatigue"

The practical effect of this is consumers often call for increased privacy protection, but then quickly suffer "consent fatigue" when reading companies' privacy policies online, either accepting default settings without consideration or treating the mere existence of a privacy policy as [a sign of protection](#).

This raises the question: what effect do privacy policies really have? And, more specifically, given privacy policies are the main day-to-day visible effect of data privacy protections for most consumers, are they fit for purpose given the way they're written and the way consumers interact with them?

## **Eloquent and unreadable**

To explore these questions further, our research looked into the privacy policies of over 4,000 firms of various sizes and different industries.

Contrary to the common belief that many firms use slightly tweaked boilerplate text for their privacy policies, we found significant variation in terms of length, structure and content between different policies, even between different companies in the same industry. This indicates there are also likely to be major differences in the quality, effect and consumer value of each policy, and we set out to examine the data to find patterns and trends with this in mind.

To be of any use, a privacy policy must be understandable to the majority of consumers and be legally enforceable in terms of the protections it offers. We analysed the policies in our sample to test these two aspects, and found that things are not as most consumers would expect.

For a start, using the [Gunning Fog Index](#) of readability, we found that, to understand the median policy in terms of complexity, a consumer would need to be educated to university level or above. This suggests most people are not able to fully understand the majority of privacy policies.

What's more, we also found the most complex policies in our sample, which are the least likely to be understood by the average consumer, tended to be the most legally watertight in terms of allowing firms to utilise and share data as they wish.

## **The right direction**

What this means for consumers on a practical level depends, of course, on how firms actually use the data they gather; this was the next aspect of our findings. Taking firm size as a variable, we found larger firms are more likely to have privacy policies in the first place and to have more complex policies that are more legally enforceable.

Interestingly, though, these firms were also more likely to use cookies that siphon data off to third parties, which is precisely what consumers on the whole say they [do not want to happen](#). However, we also found other variables at play beyond firm size, further complicating the field.

Rules requiring explicit policies and consent don't necessarily change consumer behaviour or clarify how data is used

Key among these was technical sophistication, with the most technically advanced firms tending to choose shorter, less legally watertight policies, which are more often associated with processing data in-house rather than selling it off.

To some extent, these findings answer the question over regulation, proving rules requiring explicit policies and consent don't necessarily change consumer behaviour or clarify how data is used. What to do with this information, however, is a question for society as a whole, and regulators must decide whether changes need to focus on consumer education or making privacy policies less abstruse.

One thing that is clear, though, is the reality of firms' use of data often differs significantly from what consumers assume. As understanding grows as to the nature of data privacy, it will become clearer whether or not consumers find this a problem, making it easier to take the next step in bridging the gap between expectation and reality.

In this light, our findings are the first step towards a deeper analysis of data privacy. In a commercial world in which data is heralded as ["the new oil"](#), this stands to benefit consumers and firms alike in terms of increasing knowledge and understanding.

*This article draws on findings from the paper ["The Market for Data Privacy"](#) by Tarun Ramadorai, Antoine Uettwiller and Ansgar Walther (Imperial College London).*

## **Written by**

[Tarun Ramadorai](#)

## **Published**

13 November 2019

## Category

[Technology](#)

## Key topics

[Consumer Behaviour](#), [Data Privacy](#), [Technology](#)

[Download PDF](#)

## Share



## About Tarun Ramadorai

Professor of Financial Economics

Tarun Ramadorai is Professor of Financial Economics at Imperial College London. He has a broad range of research interests in the areas of household finance, asset pricing, and international finance. He is greatly interested in finance and economics issues in emerging markets, with a particular focus on India.

You can find the author's full profile, including publications, at their [Imperial Professional Web Page](#)