BIS

BIS Bulletin

No 42

Whom do consumers trust with their data? US survey evidence

Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster and Kelly Shue

27 May 2021

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed here are those of their authors and not necessarily the views of the BIS, the Swiss National Bank, the Federal Reserve Bank of New York or the Federal Reserve System. The authors are grateful to Leo Goldman, Gen Li and Giulio Cornelli for excellent analysis and research assistance, to Martin Hood for editorial review and to Louisa Wagner for administrative support.

The editor of the BIS Bulletin series is Hyun Song Shin.

This publication is available on the BIS website (www.bis.org).

ISSN: 2708-0420 (online)
ISBN: 978-92-9197-475-6 (online)

Olivier Armantier Olivier.Armantier@ny.frb.org
Sebastian Doerr Sebastian.Doerr@bis.org
Jon Frost Jon.Frost@bis.org
Andreas Fuster Andreas.Fuster@snb.ch
Kelly Shue Kelly.Shue@yale.edu

Whom do consumers trust with their data? US survey evidence

Key takeaways

- *In a recent survey, US households say they are more likely to trust traditional financial institutions than government agencies or fintechs to safeguard their personal data. They have far less trust in big techs.*
- *This pattern differs across demographic groups: respondents from racial minorities have less trust in financial institutions, while younger respondents trust fintechs relatively more. Female, minority and younger respondents are more concerned about implications of data-sharing for their personal safety.*
- *A quarter of respondents say Covid-19 made them less willing to share data. In this group, nearly half became less willing to share with big techs. Concerns centred on identity theft and abuse of data.*
- *As the economy becomes increasingly digital, and new players expand further into financial services, strong data protection policies will become more important to shield consumers from these harms.*

Personal data lie at the heart of the digital economy. Recommendations for online shopping, personalised financial advice or credit increasingly rely on users' digital footprints (Berg et al (2020)). Large technology companies (big techs) are muscling their way into payments and lending, leveraging the vast amounts of personal data they have collected in other business lines. The Covid-19 pandemic has accelerated these trends, forcing many employees to work remotely and consumers to shop online (Alfonso et al (2021)). The resulting increase in online activity makes personal data even more abundant, and more valuable.

Currently, companies often collect and analyse these personal data without consumers' explicit consent or full understanding. While the analysis of such data can benefit consumers through improved movie recommendations or better targeted online ads, not everybody is equally comfortable with sharing their data. Rather, this unrestrained collection of personal data represents an unprecedented erosion of consumer privacy, raising important concerns around data abuse and even personal safety – even if the degree of these concerns may vary across different segments of society.

This Bulletin focuses on the willingness of consumers to share data and trust in different actors, based on a representative high-quality survey of US household heads. It assesses Americans' trust in different counterparties to safely handle their data – governments, traditional financial institutions (FIs), fintechs and large technology firms (big techs) – according to differences in the respondents' gender, ethnicity and age. The Bulletin also investigates how Covid-19 has changed attitudes and concerns towards privacy. It concludes by discussing the implications for data privacy and digital identity in financial services.

The Survey of Consumer Expectations

We investigate the attitudes towards data privacy of Americans in the Survey of Consumer Expectations (SCE). The SCE is a high-quality monthly, internet-based survey produced by the Federal Reserve Bank of New York. Launched in 2013, it is used extensively to help researchers and policymakers understand how expectations are formed and how they affect consumer behaviour. The SCE is a 12-month rotating panel

of roughly 1,300 nationally representative US household heads. New respondents are drawn each month to match demographic targets from the American Community Survey, and they stay on the panel for up to 12 months before rotating out. The survey's main aim is to collect expectations for a wide range of economic outcomes (eg inflation, income, spending, household finance, employment and housing). The survey includes a wealth of detailed demographic information, including the respondent's gender, race, age, income, education, financial literacy and willingness to take risks (Armantier et al (2017)).

To understand how consumers value their data privacy, what determines their willingness to share data and how much they trust different counterparties, the September 2020 survey contained an additional module. The module asked detailed questions on respondents' attitudes towards data privacy, for example how much they trust different counterparties to safeguard their data, and how the Covid-19 pandemic has affected these attitudes. In what follows, we use this information to investigate how consumers' attitudes towards and concerns about privacy differ across demographic groups and whether they have changed in response to the pandemic.[1]

Whom do consumers trust to safeguard their data?

The general level of trust expressed by respondents differs across counterparties, ie big techs, government agencies, fintechs and traditional financial institutions (Graph 1, left-hand panel). Respondents report the lowest trust in big techs (large technology companies such as Amazon, Apple, Facebook or Google) to safely store their personal data, ie their bank transaction history, geolocation or social media data. The median respondent assigned a value of 2 on a scale of 1 ("no trust at all") to 7 ("complete trust"), and three quarters of all respondents chose a value in the range of 1–3. Over one third of respondents reported no trust at all, while only 12% of respondents reported high trust, ie a value of 5 or higher. A meagre 1.4% of respondents reported complete trust.

Trust in a government agency (ie the federal and local governments) and in fintechs (technology firms that specialise in financial services, such as PayPal, Venmo or Quicken Loans) was higher, with the median respondent reporting a value of 4. Interestingly, reported trust in these actors exhibits higher dispersion than for big techs: while around 25% of respondents reported a level of trust of 5 or higher, another 25% reported a level of 2 or lower. For both counterparties, less than 5% of respondents reported complete trust and around 20% selected a value of 1, ie no trust at all. These numbers indicate that a sizeable share of the population has relatively low trust in the government or fintechs.

Reported trust was highest among traditional FIs. About 60% of respondents report having a high degree of trust, ie a score of 5 or higher, with a median value of 5. Over 75% of all respondents assigned traditional FIs a trust value of at least 4, and over 25% a value of 6 or higher (as indicated by the whiskers that reflect the 25th and 75th percentile of the distribution).

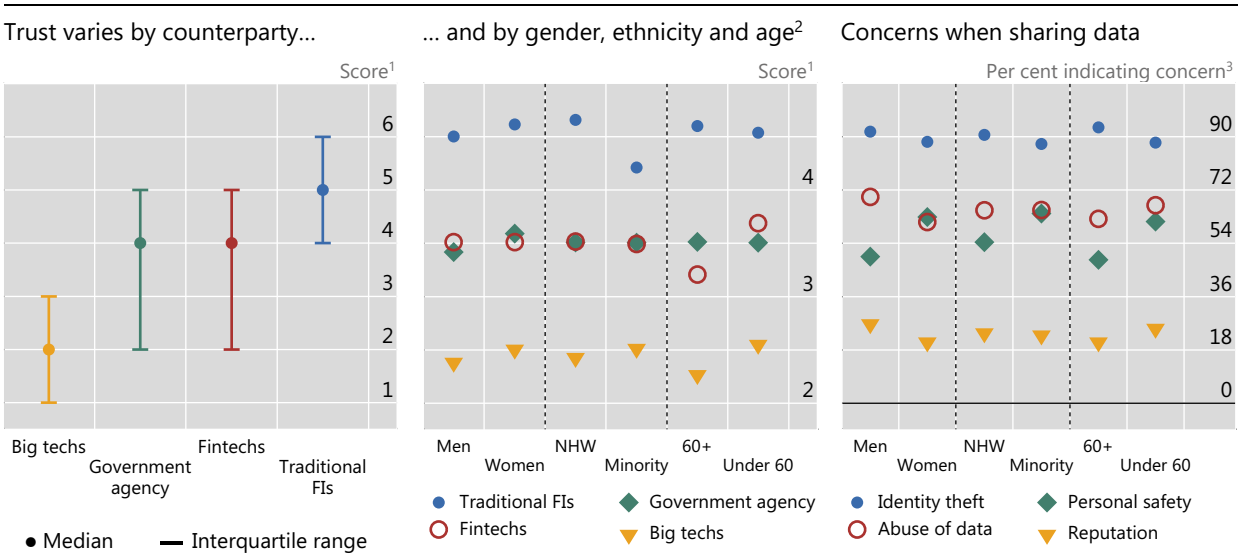
Taken together, these results indicate that consumer trust traditional FIs most to safeguard their data, while big techs are met with the most scepticism. Government agencies and fintechs lie in the middle.

Trust in these counterparties also differs by gender, race or ethnicity and age. For example, women report a slightly higher trust in financial institutions, government agencies and big techs than men do (Graph 1, centre panel). Women's trust in the fintechs is similar to that of men. A striking pattern is that respondents from a racial or ethnic minority report significantly lower trust in traditional FIs than do non-Hispanic white respondents (with average values of 4.2 and 4.7, respectively). This could relate to negative past experiences with financial institutions (see Baradaran (2015); Fu (2021)). Yet minority respondents place a somewhat higher trust in big techs, while there are no differences for government agencies and fintechs. Relative to younger cohorts, respondents aged 60 and over report higher trust in traditional FIs, but significantly lower trust in fintechs and big techs, possibly reflecting concerns about the use of new technology (Vaportzis et al (2017)). There is no difference across age groups in trust in government

[1] The sample used in this Bulletin contains 1,361 respondents, of whom 50% are female, 80% are non-Hispanic whites and 34% are 60 years or older. In the population at large, 51% are female, 63% are non-Hispanic whites and 22% are 60 years or older.

agencies. Overall, these patterns suggest that, while the overall ranking of different counterparties in terms of trust is similar across demographic groups, their trust in traditional FIs, big techs and other players can differ substantially.

Respondents' trust in counterparties to safeguard their data — Graph 1



NHW = non-Hispanic white.

[1] On a scale of 1–7, where 1 = "no trust at all" and 7 = "complete trust". [2] "Minority" comprises respondents who identify as Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or Other Pacific Islander, Other or of Hispanic, Latino or Spanish origin. "Non-Hispanic white" (NHW) comprises respondents who identify as "white" but are not of Hispanic, Latino or Spanish origin. Multiple answers possible. [3] Share of respondents that answered yes to the question "What are you specifically concerned about if your personal data were to become publicly available?".

Source: Armantier et al (2021).

All respondents appear particularly worried about identity theft.[2] When asked about specific concerns if personal data were to become publicly available, around 90% in each demographic group report that identity theft is an important issue (Graph 1, right-hand panel). Abuse of personal data for unintended purposes (in the news or media, eg for political agenda or targeted ads) is also a highly relevant concern, and more so for men and younger respondents. Notably, female, minority and younger respondents appear more concerned about implications of data-sharing for their personal safety.[3] Respondents were consistently the least worried about negative effects on their personal reputation, with around 20% of respondents selecting this answer.[4]

Has the Covid-19 pandemic affected consumers' willingness to share data?

The Covid-19 pandemic has led to a reported decline in the willingness to share personal data. A quarter of respondents said that the recent Covid-19 (coronavirus) pandemic had made them less willing to share personal data in general.[5] This reached 32% for female and 37% for minority respondents (Graph 2, left-hand panel). With 27% and 29%, older and younger respondents saw a similar change. Only 3% of those

[2] Identity theft has become a salient concern, with far-reaching risks to individuals (Reurink (2018)).

[3] This could reflect, for instance, the perceived risk of violence by an (ex-)partner, or of violence based on race or ethnicity.

[4] Notably, differences in the survey results between respondents by income or education level were much smaller than the differences by gender, race or ethnicity and age.

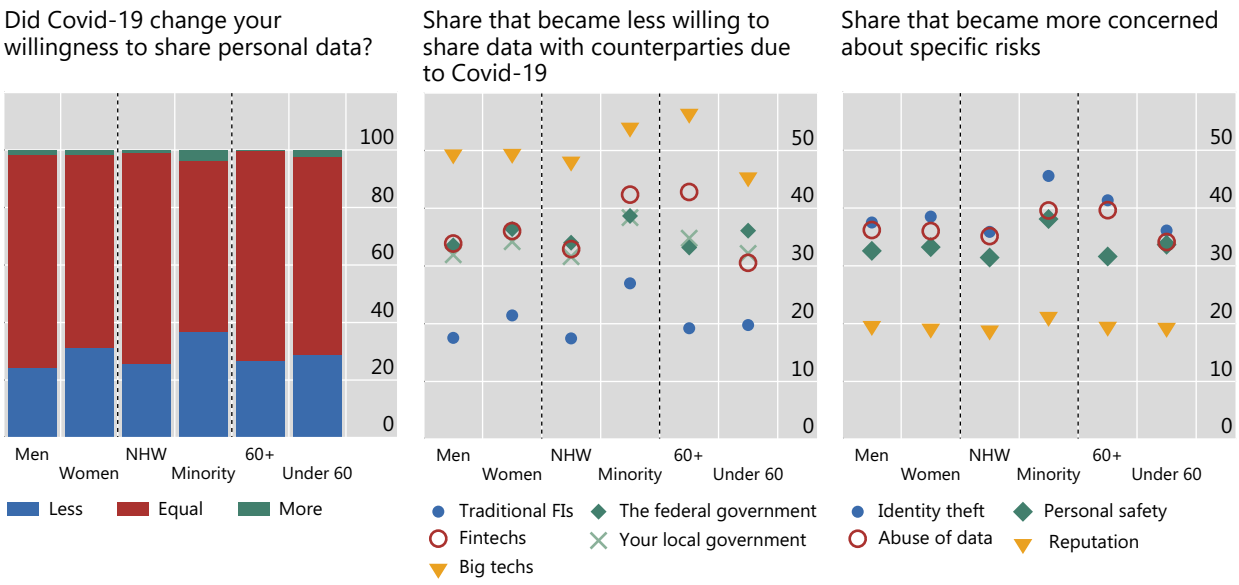
[5] The question specified that "personal data" means "*your bank transaction history, geolocation or social media data; it does NOT include your social security number, credit card info, or passwords.*"

surveyed said the pandemic has made them more willing to share personal data. In the light of the findings above, these results suggest that the pandemic has exacerbated pre-existing patterns, as female and minority respondents reported being less willing to share data to begin with.

This conclusion is reinforced when we look at different counterparties. Of respondents who said the pandemic had made them less willing to share data, nearly half said they were less willing to share with big techs, the least-trusted counterparty in general (Graph 2, centre panel). This pattern is similar for men and women, but reaches 55% for minority respondents and 56% for older cohorts. Views toward fintechs show a similar pattern, but numbers are lower on aggregate. Individuals' willingness to share data with the local and federal government saw similar declines across groups. By contrast, there was only a modest increase in the share of respondents who became less willing to share data with traditional FIs; this increase was more pronounced for minorities, the group that also reported lowest trust in traditional FIs in general.

Respondents became less likely to share data during the pandemic

In per cent of respondents — Graph 2



NHW = Non-Hispanic white.

Source: Armantier et al (2021).

When asked about the reasons for the decline in their willingness to share data, respondents reported several specific concerns. Greater concerns about identity theft ranked highest, followed by concerns about the abuse of data and personal safety (Graph 2, right-hand panel). Minority respondents in particular reported that these concerns are important drivers. Among respondents aged 60 and over, concerns about the abuse of data were more important than for younger cohorts as a reason to be less willing to share data. Only a small share of respondents reported reputational concerns, and this share was similar across all groups. Generally, Covid-19 has made respondents more worried about risks that were already salient.

International context

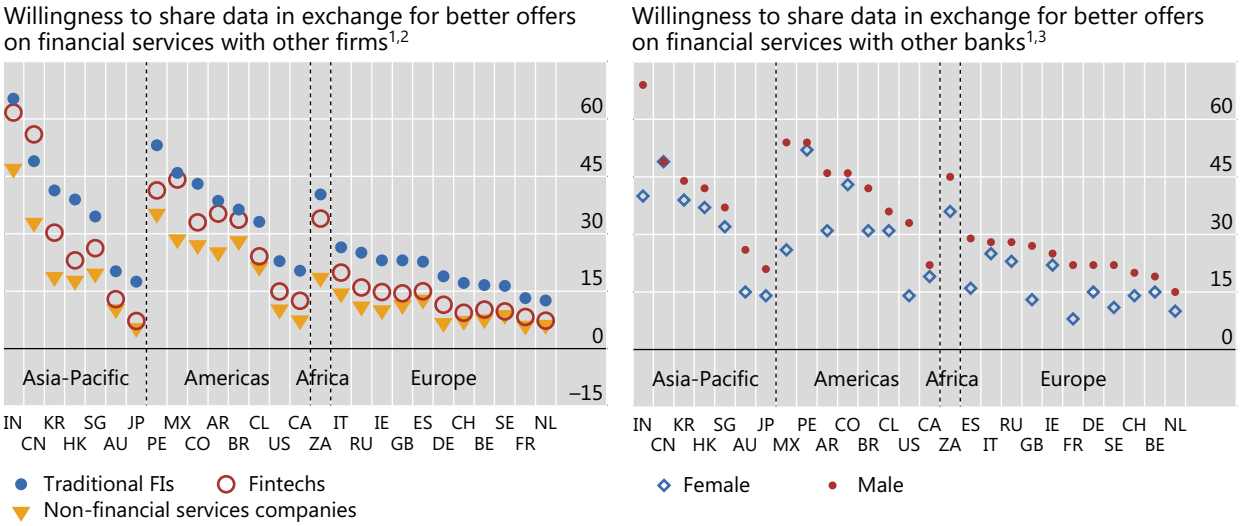
Chen et al (2021) show that the willingness to share personal data differs across counterparties and characteristics in other countries, too (Graph 3, left-hand panel). Individuals are more likely to share their data with traditional FIs than with fintechs. They are least likely to share their data with non-financial services companies, which includes big techs. The overall willingness to share data varies widely.[6] Evidence

[6] Moreover, it may be that the specific concerns for why consumers do not want to share their data differ across jurisdictions.

further suggests that women are less willing to share personal financial data than men in most countries (right-hand panel). Women also report worrying more about their security when dealing with companies online. In line with other studies (Fernandez Vidal and Medine (2019); Cruijsen (2020); Tang (2020)), the willingness to share financial data also declines with age.

The willingness to share data across counterparties and genders varies by country

As a percentage of respondents willing to share data — Graph 3



[1] Survey of 27,000 respondents in February–March 2019. For Belgium, the figure covers both Belgium and Luxembourg. [2] The question reads "I would be comfortable with my main bank securely sharing my financial data with other organisations if it meant that I received better offers from a) other traditional financial intermediaries, b) fintech companies, c) non-financial services companies". [3] The question reads "I would be comfortable with my main bank securely sharing my financial data with other organisations if it meant that I received better offers from other financial intermediaries".

Source: Chen et al (2021).

Policy implications

The digital economy creates abundant data – be it through the use of social media, online shopping, or consumers' online search queries. The Covid-19 pandemic has led individuals to rely even more on digital technologies, and particularly on big techs – the counterparty they trust least with their personal data. Going forward, these developments mean that concerns around data privacy may become more pressing. The widespread collection and use of personal data – often without the consumer's full understanding or explicit consent – could represent an unprecedented erosion of consumer privacy. This raises important questions about possible price discrimination, the concentration of market power and data abuse.

In response to these concerns, public authorities are taking actions that help address these concerns. In many countries, legislatures are defining data privacy rules, such as the EU General Data Protection Regulation or California Consumer Privacy Act.[7] Dedicated data protection authorities are implementing rules to protect sensitive personal data.[8] Central banks and financial regulators have set restrictions on the use of personal data in open banking and payments (Doerr et al (2021)). Central banks are further discussing which parties could access transaction data in the design of central bank digital currencies

[7] In some cases, voters have approved data privacy rules directly, eg California Proposition 24 on additional privacy rights or Massachusetts Question 1 initiative on access to remote data from motor vehicles for insurance purposes, both in late 2020. In contrast, the SwissID proposal in Switzerland for a private sector digital ID was resoundingly rejected in a referendum.

[8] For an overview, see https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/.

(Carstens (2021)). In addition, who should provide and manage a digital ID – the private or public sector, or a public-private partnership – remains an open question.

In each of these areas, it will be important to better understand households' specific concerns and how these differ across groups and countries. As this Bulletin has shown, there are large disparities across demographic groups in the willingness to share personal data with different counterparties and the associated concerns about negative personal consequences. The digital shift during the pandemic might thus impose disproportionate harms on some groups, which may also lead to differences in digital adoption. Understanding and addressing these concerns through sensible regulation is essential if digital technologies are to be used in a safe and inclusive way for all in society.

References

Alfonso, V, C Boar, J Frost, L Gambacorta and J Liu (2021): "E-commerce in the pandemic and beyond", *BIS Bulletin*, no 36, January.

Armantier, O, G Topa, W Van der Klaauw and B Zafar (2017): "An overview of the survey of consumer expectations", *Economic Policy Review,* vol 23, no 2, pp 51–72.

Armantier, O, S Doerr, J Frost, A Fuster and K Shue (2021): "Nothing to hide? Survey evidence on who is willing to share their data", mimeo.

Baradaran, M (2015): *How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy*, Harvard University Press.

Berg, T, V Burg, A Gombović and M Puri (2020): "On the rise of fintechs: credit scoring using digital footprints", *The Review of Financial Studies*, vol 33, no 7, pp 2845–97.

Carstens, A (2021): "Digital currencies and the future of the monetary system", speech at the Hoover Institution, 27 January.

Chen, S, S Doerr, J Frost, L Gambacorta and H S Shin (2021): "The fintech gender gap", *BIS Working Papers,* no 931.

Cruijsen, C van der (2020): "Payments data: do consumers want banks to keep them in a safe or turn them into gold?", *Applied Economics*, vol 52, no 6, pp 609–22.

Doerr, S, L Gambacorta and J M Serena Garralda (2021): "Big data and machine learning in central banking", *BIS Working Papers,* no 930.

Fernandez Vidal, M and D Medine (2019): "Is data privacy good for business?", *CGAP Focus Note*, Consultative Group to Assist the Poor, Washington DC, December.

Fu, I (2021): "The Freedman's Bank and the Persistence of Mistrust", mimeo.

Reurink, A (2018): "Financial fraud: a literature review", *Journal of Economic Surveys*, vol 32, no 5, pp 1292-325.

Tang, H (2020): "The value of privacy: evidence from online borrowers", mimeo.

Vaportzis, E, M Giatsi Clausen and A Gow (2017): "Older adults' perceptions of technology and barriers to interacting with tablet computers: a focus group study", *Frontiers in Psychology,* no 8(1687).

Previous issues in this series

No 41 12 April 2021	Futures-based commodity ETFs when storage is constrained	Sirio Aramonte and Karamfil Todorov
No 40 25 March 2021	Liquidity to solvency: transition cancelled or postponed?	Ryan Banerjee, Joseph Noss and Jose Maria Vidal Pastor
No 39 17 March 2021	Liquidity management and asset sales by bond funds in the face of investor redemptions in March 2020	Andreas Schrimpf, Ilhyock Shim and Hyun Song Shin
No 38 10 March 2021	Covid-19 bank dividend payout restrictions: effects and trade-offs	Bryan Hardy
No 37 14 January 2021	Covid-19 and cyber risk in the financial sector	Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta and David Whyte
No 36 12 January 2021	E-commerce in the pandemic and beyond	Viviana Alfonso, Codruta Boar, Jon Frost, Leonardo Gambacorta and Jing Liu
No 35 15 December 2020	The recession-mortality nexus and Covid-19	Sebastian Doerr and Boris Hofmann
No 34 14 December 2020	Central bank swap lines and cross-border bank flows	Iñaki Aldasoro, Christian Cabanilla, Piti Disyatat, Torsten Ehlers, Patrick McGuire and Goetz von Peter
No 33 02 December 2020	What comes next? Recovery from an uneven recession	Daniel Rees
No 32 12 November 2020	Monetary policy response in emerging market economies: why was it different this time?	Ana Aguilar and Carlos Cantú
No 31 09 October 2020	Bankruptcies, unemployment and reallocation from Covid-19	Ryan Banerjee, Enisse Kharroubi and Ulf Lewrick
No 30 09 October 2020	The outlook for business bankruptcies	Ryan Banerjee, Giulio Cornelli and Egon Zakrajšek
No 29 14 August 2020	Bonds and syndicated loans during the Covid-19 crisis: decoupled again?	Tirupam Goel and Jose Maria Serena
No 28 23 July 2020	Inflation at risk from Covid-19	Ryan Banerjee, Aaron Mehrotra and Fabrizio Zampolli

All issues are available on our website www.bis.org.