

A blue smartphone is placed inside a metal bowl filled with red and white peanuts. The phone's screen displays the time 05:06 and the date 05 07 2018. The background is a close-up of the peanuts in the bowl.

MAKING DATA WORK FOR THE POOR

New Approaches to
Data Protection and Privacy

Consultative Group to Assist the Poor

1818 H Street NW, MSN F3K-306

Washington, DC 20433 USA

Internet: www.cgap.org

Email: cgap@worldbank.org

Telephone: +1 202 473 9594

Cover photo by Geoffrey Buta, CGAP Photo Contest 2018.

© CGAP/World Bank, 2020

RIGHTS AND PERMISSIONS

This work is available under the Creative Commons Attribution 4.0 International Public License (<https://creativecommons.org/licenses/by/4.0/>). Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the terms of this license.

Attribution—Cite the work as follows: Medine, David, and Gayatri Murthy. 2020. “Making Data Work for the Poor: New Approaches to Data Protection and Privacy.” Washington, D.C.: CGAP.

All queries on rights and licenses should be addressed to CGAP Publications, 1818 H Street, NW, MSN F3K-306, Washington, DC 20433 USA; e-mail: cgap@worldbank.org.

EXECUTIVE SUMMARY

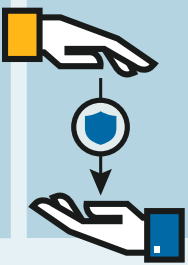
A S THE COMMERCIAL USE OF PERSONAL DATA GROWS exponentially, so do concerns over whether that data will be used in consumers' best interests. This is particularly true for financial services in emerging economies, where data expand the potential for reaching poor and underserved communities with suitable products but where customer protection risks are great. In many markets ranging from Indonesia to India and Kenya, it is unfair to impose the burden of consent on individuals to protect their data when such a large proportion of the population are opening accounts or coming online for the first time, literacy rates are low, and individuals face potential language and technological barriers.

Many countries are considering comprehensive legislation to protect people's data and privacy across all sectors and services. The European Union's General Data Protection Regulation (GDPR) is the most well-known effort in this regard. Countries as diverse as Ghana, South Africa, India, Indonesia, Kenya, and even the United States are considering or have passed wide-ranging data protection legislation.

Yet data protection regimes rely heavily on individual consumer consent. This places an unreasonable burden on low-income customers. For example, it is unrealistic even in developed countries for customers to read all the disclosure documents for all the apps on their smartphone. CGAP has concluded that the consumer consent model is broken, additional protections are necessary to protect consumers, and protections can be introduced in ways that do not inhibit responsible innovation. Accordingly, we make three policy recommendations.


CGAP's Three Recommendations

1




Shift Onus Onto Provider
Place new responsibilities onto data collectors and processors, rather than relying on consumer consent. Two options:

Legitimate Purposes Test
Only allowed to use data in ways that benefit the customer;



OR

Fiduciary Duty
Must always act in the interests of the customer.




2



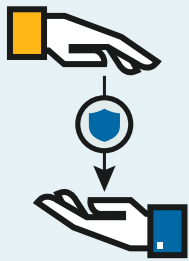
Digital Bill of Rights
Empower consumers to control their own data by allowing them to easily access, correct and port data free of charge.

3



Privacy Representatives
Ensure fairness in processing of data through privacy representatives who can review consumers' data profiles and check algorithmic models for fairness, bias and exclusion.

1. Shift the Onus of Protection onto Providers



The burden of data privacy should shift from individuals to providers. Providers should be responsible for using data only for legitimate purposes and in a manner that serves customers' interests. Two alternatives are addressed in this paper.

One approach, a legitimate purposes test, limits use of data to what is compatible, consistent, and beneficial to consumers, while allowing firms to use de-identified data to develop new and innovative products and services. A key feature of a legitimate purposes approach is that it cannot be overridden by obtaining individual consent. In other words, everyone benefits from legitimate purposes protections, regardless of which boxes they are required to check before accessing a website, downloading an app, or using a digital service.

A legitimate purposes test enables providers to use an individual's data to service accounts, fulfill orders, process payments, collect debts, control for quality, enforce security measures, or conduct audits. Innovative uses of data would be permitted if they are consistent with the service for which the data were initially collected. Going beyond such uses, data could be used for more wide-ranging purposes if they were robustly de-identified to reduce the risk of them being used in ways that are harmful to the individuals who provided these data.

An alternative approach, a fiduciary duty requirement, requires data collection and processing firms to always act in the interests of, and not in ways detrimental to, the subjects of the data. Such legislation, which is currently being considered in the United States and India, would mean that providers could not use data in ways that benefit themselves over their customers, or sell or share customers' data with third parties that fail to put the customers' best interests first. This approach would limit the information asymmetry in many markets in which providers have a much greater knowledge than their customers about how customers' data may be used. The fiduciary duty approach also recognizes that poor people should not be required to give up their data protection rights to use digital services. Instead, legally obligating providers to act in the best interest of their customers can help establish trust and confidence among customers that their data are being used responsibly, making them more willing to use new products and services.



2. Empower Users through Modern Digital Rights That Go Beyond Consent

Our second policy recommendation calls for adopting a set of six digital rights that empower consumers to access, review, and correct their data and to transfer their data to other providers. Most of these rights should be enforced not only at the beginning of a service or relationship, but even after customer data have been collected or processed.



3. Ensure Fairness in Processing Through Privacy Representatives

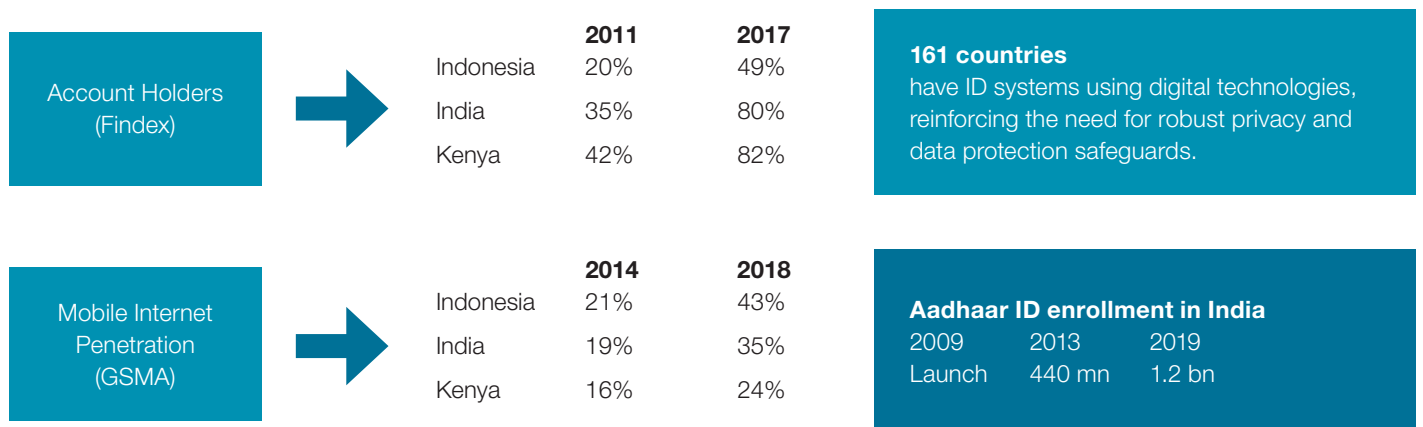
As artificial intelligence (AI) becomes increasingly complex and widespread, we need to counter the danger that algorithmic or machine learning reinforces exclusionary biases. Otherwise AI could increase economic inequalities rather than counter them. Moreover, AI-driven decisions are beyond the individual's ability to monitor and evaluate. Consumers need expert assistance in assessing how automated decisions are made. Privacy representatives, whether persons or digital mechanisms, should be introduced to assess decision-making models for fairness, bias, and exclusion. This may not seem pertinent today in most emerging markets, but it will soon become a critical tool to prevent exclusion as products are introduced that use AI and machine learning to assess who is eligible and on what terms are introduced.

Protecting data is critical to developing trust and confidence among poor consumers and to building a truly inclusive digital economy. Data can be used to lift up and benefit the lives of poor people, but they must not be used to exacerbate exclusion and inequality. Outdated reliance on consumer consent cannot provide adequate protections. We need to begin work on new approaches and foundational rights that are future ready.

THE PROLIFERATION OF PERSONAL DIGITAL DATA

IN MANY DEVELOPING COUNTRIES, THE EXPANSION OF NEW ID systems, access to digital financial services, and the deeper penetration of mobile devices are pulling more and more people into the digital economy, rapidly expanding the size of the digital data trails they leave behind. Consider three fast-moving countries: Indonesia, India, and Kenya. As Figure 1 shows, mobile Internet penetration and financial account access are increasing side by side.

FIGURE 1. **Increase in low-income populations joining the digital economy**



Sources: Findex (World Bank), GSMA, Identification for Development (World Bank).

These developments are unlocking new opportunities to use data analytics to provide access to financial services for the underserved. Many poor people lack formal financial records or credit histories and hence often are excluded, but data analytics provide alternate means of assessing eligibility for financial products. This may also lead to lower prices, greater competition and choice, and more useful, customized services. Data can expand financial inclusion in many ways, including through alternative credit scoring, links to application programming interfaces (API), big data or public data analytics, and automated claims processing.

Alternative credit scoring. Digital credit products, whether for individuals or micro, small, and medium enterprises (MSMEs), collect data from alternative and online sources. These include electronic bank accounts, payments gateways, online accounting companies, and e-commerce marketplaces. Using these data, financial institutions can create alternative credit scores and offer faster and more customized loans. Firms like Branch and Tala are prominent examples of firms offering microloans in Africa and South Asia using various types of data from smartphones. See Box 1.

Application programming interfaces (APIs) links. New fintech and technology companies can expand data sharing by using the APIs of banks or mobile money companies to offer products such as insurance, investments, or other services

based on payment behavior.¹ Use of open APIs may result in fintech innovation that can give underserved people access to new products and services. Examples range from leased tractors to pay-as-you-go solar to financial health apps.

Big data or public data analytics. Data can be valuable when they come in large quantities that can be observed over time. For example, insurance providers use satellite and yield data to reduce the cost of offering insurance to smallholder farmers.

Automated claims processing. Though not yet widespread in financial services in emerging markets, algorithms and other digital processing will increasingly be used to assess, approve, and disburse claims for insurance.

But as the commercial use of personal data grows exponentially, so do concerns over whether that data will be used in the consumers' best interests.

Algorithms and artificial intelligence (AI) are being used to make decisions about customers, such as whether they will get a loan or whether their insurance claims should be paid in a way that is consistent, accurate, and scalable. But there is also the risk that bias or unfairness in such models will entrench exclusion around socioeconomic status, gender, race, or caste at scale.

BOX 1. **Examples of firms using alternative credit scoring**

Tala uses a smartphone app to evaluate applicants' credit risk. It gathers various types of data, including where loan applicants spend their time, how many people they communicate with every day, how often they call their parents (by searching call logs for the word "mama"), and less surprisingly, whether they pay their bills on time.

Branch makes lending decisions using information stored on smartphones, including call logs, SMS logs, Facebook friends, contact lists from other social media accounts, photos, videos, and other digital content.

Fintechs such as **Yoco** in South Africa and **Aye Finance** in India make noncollateralized loans to MSMEs based on data from the firms' digital payments and transactions.

1 An API allows one software program to "talk" to another. APIs enable a wide range of innovative products and services that millions of people use every day. For instance, ride-hailing apps use APIs to leverage other companies' mapping and payments systems. When a financial services provider "opens" its APIs, it makes them widely available to other companies. To learn more about the possibilities of open APIs, see "Open APIs in Digital Finance," CGAP, <https://www.cgap.org/topics/collections/open-apis>.

BOX 2. Recent approaches to data protection legislation

Countries have taken different approaches to data protection, including sectoral versus omnibus laws. Notable examples include the following:

- The **European Union's** GDPR applies broadly. Its features include a focus on consumer rights, reliance on consumer consent with a legitimate use constraint, and a duty to build in privacy as products are designed.
- The **United States** uses a sectoral approach, in which consent plays a significant role. It includes a health privacy law (Health Insurance Portability and Accountability Act), laws focusing on data protection within credit bureaus, and privacy laws pertaining to children, video rentals, and drivers' records. Several approaches to comprehensive privacy legislation are now being considered, some of which would rely on consent.
- **India** has a draft personal data protection bill framed as an omnibus law that would create a separate data protection authority. The law relies on consumer consent, but it also highlights the concept of "data fiduciaries." Under Indian law, a fiduciary relationship is "a relationship in which one person is under a duty to act for the benefit of the other."
- In the past decade, several Asian countries, including the **Philippines** and **Thailand**; several African countries, including **South Africa, Ghana, Senegal, and Kenya**; and several Latin American countries, including **Mexico** and **Chile**, have introduced omnibus data protection laws and/or began enforcing them.

Personal data can be leaked, stolen, or exposed through security breaches that can result in identity theft or embarrassment (Baur-Yazbeck 2018). Attempts to hack financial firms, including those that provide financial services to poor people, have the potential to effect devastating losses to vulnerable populations, which can undermine trust and confidence.

Customers in emerging markets, especially those who are underserved and poor, who are going digital for the first time may have limited literacy or experience with technology, making them ill-equipped to protect their data.

Recognizing this, many countries, whether developed, emerging, or developing, have been considering comprehensive legislation to protect people's data and privacy across all sectors and services (see Box 2). The European Union's General Data Protection Regulation (GDPR), which took effect in May 2018, is one of the most well-known efforts in this regard, but countries as diverse as Ghana, South Africa, India, Indonesia, Kenya, and even the United States are considering or have passed wide-ranging data protection legislation. There is no one approach, with some data protection laws applying across the economy while others employing a sector-by-sector approach.

THE PROBLEM: RELIANCE ON CONSENT DOES NOT PROTECT CONSUMERS

MOST DATA PROTECTION LEGISLATION, WHETHER PASSED OR pending, are based on the prevailing “consent” model. This model posits that once someone has been presented with a privacy notice and then consents or ticks a box saying, “Yes, I agree to the Terms and Conditions,” it means that they fully understand what will happen to their information and they have given their informed consent, putting them in control of how their data will be used and disclosed.

In theory, individuals decide where their data go and what is done with them. This concept is appealing because it has the aura of individual agency. In practice, whatever is stated in

a provider’s privacy policy usually dictates use and disclosure of personal—sometimes sensitive—information. Importantly, the consent model absolves much of a firm’s responsibility for proper data handling.

The average smartphone owner has 80 apps on her phone each month; most of the apps have corresponding privacy notices, yet almost no one reads them—and if we did, it would take a lot of time.

(App Annie 2018)

Few people read or understand consent notices. When accessing a new digital service, we are nearly always asked to confirm that we have read and agree to terms and conditions. Several studies show this is far from what happens. A recent Deloitte survey of 2,000 U.S. consumers found that 91 percent of people consent to legal terms and service conditions without reading them (Cakebread 2017). For young people, ages 18 to 34, the rate is even higher, with 97 percent agreeing to conditions before reading. Fewer than 2 percent of Microsoft customers have used its Privacy Dashboard, and of the 2.5 billion visits to Google’s accounts page, only 20 million people or a similar small percentage changed their ad targeting preferences or turned off ad targeting altogether (Ng 2019).

Even if someone were to diligently and carefully read privacy notices, research shows it would take that person 76 days to read all the relevant notices (Madrigal 2012).



**BOX 3. Limitations of consumer consent:
Evidence from India**

A 2018 study by the National Institute for Public Finance and Policy (NIPFP) shows that even well-educated people do not understand privacy notices. This study began by testing how well urban, English-speaking, college and law students understand the privacy policies of five popular Indian technology companies: Flipkart, Google, Paytm, Uber, and WhatsApp. How did they do? Not very well.

The students scored an average of 5.3 on a scale of 10, doing worse in areas where the policy terms were unclear or required the reader to make his or her own inferences. They fared even worse on policies that had the most unspecified terms or were long. They were also unable to understand key legal terms such as “third party,” “affiliate,” and “business partner.”

In a second step of the study, NIPFP had the policies evaluated by experts. Most found the policies poorly drafted and a check-the-box compliance exercise. Most policies were available only in English, which is not read by many Indians. And most policies scored between 16 and 41 on the Flesch-Kincaid readability score, which suggests readers need graduate-level reading skills—this in a country where 8.2 percent of Indians age 15 and above have an education level of high school graduate or above.

Source: Bailey et al., 2018.

Privacy notices are often long, complex documents written by companies’ legal teams to ensure that the companies limit their liability and are protected against regulatory scrutiny. In other words, privacy notices are generally written to protect the interests of firms rather than to inform or help consumers make better choices.

“Better notices” are not likely to work any better. Some regulators and companies have experimented with ways to make privacy notices more customer centric and empowering. Solutions have included rewriting long notices as a series of small chunks of information and asking for consent at more relevant times, such as when data are about to be shared, transmitted, or processed, as opposed to before a service is accessed (Schaub 2017). An example of the latter approach is when Facebook asks users to consider sharing settings for their pictures just before posting. While this approach is sometimes successful in making people think before they click, it is unclear whether it changes behavior in a meaningful way. Companies’ information practices are often complex, which make it almost impossible to simply and briefly disclose them in notices. In some cases, deceptively simple notices have been used to justify undisclosed and widespread information sharing (Valentino-Devries et al. 2018).

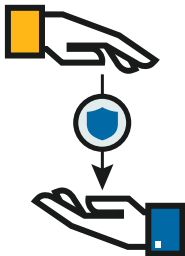
Consent is inadequate in protecting customers. New solutions may improve consent, but as the digital age progresses, the consent model is inadequate. Devices like Amazon’s Alexa that can listen to us all day at home may have our consent, but what about the guests who enter our homes and who have not consented? Cameras also frequently capture our image and movements without our consent. Advances in data sharing are making consent less feasible. If a financial institution used your location data to help determine your creditworthiness, for instance, this could mean that failing to pay attention to your phone settings could cost you a mortgage or small business loan. Consent is inadequate in three areas:

- **All or nothing.** When consumers want to download an emoji app or access an online credit service, they usually have two choices: accept the terms and conditions or don't use the service. There's usually no flexibility to negotiate an individualized contract for data use.
- **Comprehension.** People often consent to third-party sharing without fully understanding the consequences. (See Box 3.)
- **Complexity or bias.** Consent means little when customers do not understand what is being done with their data. Complicated machine-learning algorithms may combine disparate forms of personal and nonpersonal data to create deep individual profiles. People may consent to automated data processing but unknowingly subject themselves to biases or adverse decisions, exposing them to the risk of exclusion at large scale.

The idea of consent is deeply rooted in western notions of individual autonomy and liberty. It is rare for governments and companies to acknowledge that consent is an insufficient tool for data protection (Parsheera 2019). But in an encouraging sign, the Australia Competition and Consumer Protection Commission (ACCC) recommended in 2019 that the Australian government consider shifting responsibility for data protection and privacy away from consumers and toward entities collecting, using, and disclosing personal information.

CGAP's research has focused on alternatives and additions to current policy frameworks that would better protect citizens and continue innovation in financial services. The rest of the paper presents three policy recommendations to enhance data protection and examines:

1. How two alternative approaches to data protection, which go well beyond the consent model, empower the individual when it matters and impose reasonable restrictions on firms that collect and process data.
2. How digital rights that go beyond consent can be provided even after customer data have been collected or processed, and how they can empower those who are traditionally excluded or underserved by the financial system.
3. How privacy representatives can address fairness in processing data. Privacy representatives would be public or private entities that would hold algorithmic bias in check and guide consumers through the morass of company data practices.



Recommendation 1: Shift the Onus of Protection onto Providers

The inadequacy of consent and users' inability to fully read consent notices should not lead us to conclude that privacy is a less significant issue in people's minds. A 2017 qualitative study of India's Aadhaar, the national biometric identifier, stirred public debates about the appropriate use of data (Dalberg, CGAP, and Future of Finance 2017). The research showed that rural and urban residents strongly asserted their right to have personal information treated responsibly. Interviewees indicated clear and strong preferences for providers that give them agency and control over their data. A similar study by Deloitte in the United States

in 2018 showed that 73 percent of all consumers across all generations said they would be more comfortable sharing their data if they had better control of them (Loucks 2018).

Research also shows that data privacy scandals in the past five years have prompted people to adjust their data-sharing preferences, limit use, or opt out entirely from sharing their data where they felt a lack of trust. People are realizing that their consent may have enabled their lack of privacy in some cases. Yet it is hard to imagine that the world will completely abandon some form of consent in data protection policy. Consent is a key element of autonomy. Even with new approaches being introduced, people would play a role in deciding what information of theirs is collected though this has its limitations due to passive data collection—that is, data not collected through the action of the individual, such as information on one’s location. There is no clear way to know where all this passive information ends up when it is taken from apps and major platforms (Warzel 2019).

The inadequacies of consent coupled with its centrality to privacy conversations mean that we must develop strong and viable alternatives to data protection in new policies. More responsibility for data protection should be shifted to the entities, whether financial institutions, fintechs, or other technology firms that collect and process data. Such an approach need not necessarily stifle innovation; in fact, it can encourage responsible innovation that creates value for customers while also protecting them. The two alternatives we present show what an approach to data protection that goes beyond consent could look like. These are (i) the legitimate purposes test and (ii) the fiduciary duty requirement between providers and consumers. By using one of these approaches, policy makers can avoid the shortcomings of the notice-and-consent model, protect individuals’ personal data, promote trust and confidence in DFS, and still leave room for DFS providers to innovate.

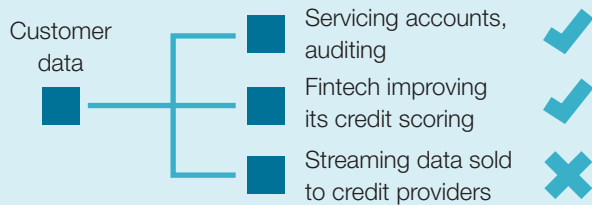
APPROACH 1. THE LEGITIMATE PURPOSES TEST

Consumers’ personal data should be processed in ways that are consistent with reasonable expectations they have formed based on their relationships with services providers (see Box 4). Providers should be limited to collecting, creating, using, and sharing data necessary for or compatible with the services being provided. Along these lines, New Zealand’s Privacy Commissioner has noted that unlike in other parts of the world, its “law does not depend on consent as the primary authority for collecting, using and disclosing personal information. Consent certainly has a role, but the main driver is the legitimate business purpose of the holder of the information” (Edwards 2019).² Hence, when the data are no longer necessary for legitimate uses, these data should not be retained in identifiable form. A key feature of a legitimate purposes approach is that it cannot be overridden by obtaining individual consent. In other words, everyone benefits from legitimate purposes protections, regardless of which boxes they were required to check before accessing a website, downloading an app, or using a digital service.

2 Unlike the approach proposed in this paper, novel use or disclosure of personal information would not be considered a breach of the principle where the company concerned “believes on reasonable grounds that the use/disclosure” is authorized by the individual concerned. Thus, in New Zealand, consent can override legitimate purposes.

BOX 4. What is the legitimate purposes test?

How does it work?



Features

Limits use to what is compatible, consistent, and beneficial to data subjects. Allows firms to process data for new, related innovations.

Calls for consumers' personal data to be processed in beneficial ways that are consistent with reasonable expectations they have formed based on their relationships with services providers.

Is not overridden by consent.

Allows data to be used for more wide-ranging purposes if robustly de-identified.

Example of how it works



A company offering loans to MSMEs collects data such as tax receipts, bank cash-flow statements, and sales and profit-loss records from the MSME. It then analyzes and scores

the data to provide fast, secure, and digital loans in India. A review of company practices reveals that the firm de-identified the data of each firm and used these data to strengthen their decision-making models.

Assessment: This is legitimate and is in the interest of customers.

how such data would be used" (Sathe 2019).³ In a legitimate purposes approach, data obtained to provide stories and songs could not also be used for scoring credit applications. Likewise, a food-purchasing app would not be permitted to share information on potato chip purchases compared to kale purchases with the customer's life insurance company.

³ Ironically, Sathe (2019) said: "It is possible that companies are compromising users' privacy on a broad scale but coming up with results that are not more accurate than traditional lending was."

Legitimate purposes for collecting and using data could include servicing accounts, fulfilling orders, processing payments, collecting debt, ensuring a site or service is working properly, controlling for quality, applying security measures, conducting an audit, and doing other activities driven by evolving business models such as introducing financial management tools. This allows providers to establish the scope of permissible data uses depending on the product or service they choose to offer. More information can be used to provide financial advice than to fulfill a request to ship a single product. A social networking site could post data so a customer's connections can see her postings. The site could also use the data to target advertising that allows the site to be offered without charge, as long as this is made clear to the customer.

The Facebook/Cambridge Analytica case that exploded on the global scene in early 2018 illustrates how easily data abuses can occur. Cambridge Analytica had harvested personal data from millions of people's Facebook profiles without their consent to target them for political advertising.

It is not the only example of data being used in unexpected ways. In India, researchers discovered that a music and storytelling app was collecting sensitive data, such as global positioning system (GPS) locations, which were used in unrelated credit scoring. HuffPost India concluded that "a user could consent to an app collecting data without knowing

Aside from any restrictions on legitimate purposes, companies' use of data would also be limited by an individual's legal or constitutional freedoms and rights. Of course, providers would also have to comply with other legal obligations and be permitted to disclose information necessary to protect someone whose health or safety was threatened. Innovative uses of data that are consistent with the service being provided would be permitted.

Data could be used for more wide-ranging purposes if they are robustly de-identified and are not used in ways that harm the data subjects. A legitimate purposes approach would permit providers to use data they collect as long as the data have been de-identified, aggregated, or stripped of personally identifiable information. Thus, the data could be used to improve the provider's business operations, develop new products and services, and improve risk assessment without impinging on customer privacy.

While much has been written about the ease of re-identifying information,⁴ in this context, efforts to re-identify could be prohibited by law both by the "data controller," typically the company with which the consumer is doing business, that makes decisions about the use of the data and any other entities that might receive the information. Several tools, including federated learning and differential privacy, can be used to ensure data privacy while promoting innovation (Pichai 2019).^{5 6} See Box 5.

4 Data re-identification or de-anonymization is the practice of matching anonymous data (also known as de-identified data) with publicly available information, or auxiliary data, to discover the individual to which the data belong to. For more, see, e.g., Ohm (2010).

5 According to Pichai (2019), federated learning "allows Google's products to work better for everyone without collecting raw data from your device. Federated learning is how Google's keyboard can recognize and suggest new words like 'YOLO' and 'BTS' after thousands of people begin typing them—without Google ever seeing anything you type."

6 "When differential privacy is used, it can be understood as (essentially) ensuring that using an individual's data will not reveal personally identifiable information specific to him or her" (Wood et al. 2018).

BOX 5. How the legitimate purposes test goes beyond GDPR and Convention 108+ protections

GDPR and Convention 108+ provide that information must be collected for explicit, specified, and legitimate purposes and not processed in a way incompatible with those purposes.^{a, b} However, there is a significant difference between requiring the uses be compatible with the purpose for which information is collected, as is the case for a legitimate purposes approach, as opposed to not being incompatible, which seems to permit a broader range of uses beyond what consumers would likely expect.

Second, the legitimate purposes approach would not allow consent to override a purpose limitation. By contrast, under GDPR, according to the U.K. Information Commissioner, purpose limitations can be overridden if “you get the individual’s specific consent for the new purpose” (ICO 2019).^c

A third key difference is that GDPR permits processing of data without consent if the data controller has a “legitimate interest.”^d This test is quite flexible, is focused on the interests of the provider and not the

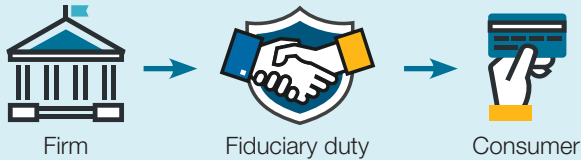
individual, and arguably is somewhat open ended.^e

In a recent case involving Google, the Australian Competition and Consumer Commission (ACCC) considered use of consent versus legitimate interest, noting that “Google submits that ‘legitimate interests’ can be an effective alternative to consent that balances the impact of data processing against the ‘legitimate interests’ of the entity processing the information. ACCC notes, however, that there is considerable uncertainty and concern surrounding the relatively broad and flexible definition of the ‘legitimate interests’ basis for processing personal information under GDPR. Therefore, ACCC does not recommend that the personal information collected, used, or disclosed based on ‘legitimate interests’ to be exempt from the proposed consent requirements” (ACCC 2019, 466).

CGAP believes data protection law should focus on the individual whose data are being collected and used and that a legitimate purposes approach would be more protective of those individual interests.

- a. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is a 1981 Council of Europe treaty that protects the right to privacy of individuals. It is an international legally binding instrument on the protection of personal data open to any country to ratify. The convention was revised and modernized in 2018. GDPR and Convention 108+ have been adopted by many countries.
- b. GDPR, Article 5(1)(b): “[C]ollected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.” It’s not clear why, but GDPR’s Recital 50, which is not binding, allows processing “only where the processing is *compatible* with the purposes for which the personal data were initially collected.” [Emphasis added.] Convention 108+, Article 5(4)(b): “[C]ollected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes.”
- c. See, also, letter from the Dutch Data Protection Authority on 1 July 2019 to the Dutch Banking Association, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/compliancebrief_nvbnvb.pdf (per Google translate: further processing for a different purpose is permitted if “based on the consent of the person concerned”).
- d. GDPR, Article 6(1)(f). See also GDPR Article 6(4).
- e. The U.K. Information Commissioner answers the question: When might legitimate interests be appropriate? “Legitimate interests is the most flexible of the six lawful bases. It is not focused on a particular purpose and therefore gives you more scope to potentially rely on it in many different circumstances” (ICO 2018).

**BOX 6. What is the fiduciary duty requirement?
How does it work?**



Features

It requires that firms act in interests of, and not detrimental to, consumers at all times.

It is a standard expectation imposed on investment advisers, doctors, and lawyers to ensure they act in the best interests of their clients or patients.

It identifies what is considered detrimental: reasonably foreseeable and material physical or financial harm to an end user or be unexpected and highly offensive to a reasonable end user.

Example of how it works

Insurance Mart is meant to be an insurance marketplace in Argentina that recommends insurance products to customers and matches them with products that meet their needs. However, an investigation reveals that Insurance Mart accepts payments from Casa Insure, an insurance company, to recommend the insurer to customers, even though Casa has higher premiums than other companies for the same coverage.

Assessment: Not acceptable. Insurance Mart is acting in its own and Casa's interests and not the customer's.

APPROACH 2. THE FIDUCIARY DUTY REQUIREMENT

The second approach we propose protects personal data by creating a fiduciary relationship between individuals and providers (see Box 6).⁷ A fiduciary relationship generally exists where one person is under a duty to act for the benefit of the other. This duty is a standard expectation imposed on investment advisers, doctors, and lawyers so that they act in the best interests of their clients or patients. It requires them to use and disclose data for their clients' benefit. As Harvard Professor Jonathan Zittrain (2018) describes the concept: "[It] has a legalese ring to it, but it's a long-standing, commonsense notion. The key characteristic of fiduciaries is loyalty: They must act in their charges' best interests, and when conflicts arise, must put their charges' interests above their own."

The approach is being considered in India and the United States. The Data Protection Committee (n.d.) in India charged with drafting data protection legislation characterized the fiduciary duty as one in which "an individual expects that her personal data will be used fairly, in a manner that fulfils her interest and is reasonably foreseeable." A U.S. data protection bill, introduced in 2018 by 15 U.S. senators, would establish duties of care, loyalty, and confidentiality for providers. If passed, providers would

not be allowed to use data in ways that benefit themselves over their customers or sell or share customers' data with third parties that don't put customers' best interests first. Under the proposed legislation, detriment of the end user would mean practices that "result

7 "[C]ompanies have 'increasing capacities for surveillance and control' of their users, but users have little ability to monitor the companies. Users therefore worry, with good reason, that the companies will take advantage of them. To help level the playing field and allay such worries, Balkin [a law professor who has promoted the fiduciary duty approach] proposes that we draw on principles of fiduciary law that assign one actor (the fiduciary) 'special obligations of loyalty and trustworthiness' toward another actor (the beneficiary)" (Khan and Pozen 2019).

in reasonably foreseeable and material physical or financial harm to an end user” or “be unexpected and highly offensive to a reasonable end user” (Barrett 2019).

To some extent, this approach would correct the information asymmetry in many markets in which providers know much more than their customers about how customer data may be used or shared. Since it’s often difficult or impossible for customers to monitor how their data are used and disclosed, a fiduciary duty must require companies to prioritize their users’ interests over their own (see Box 7). This approach also recognizes that poor people in developing countries should not be required to give up their data protection rights to use digital services. Instead, legally obligating providers to act in the best interest of their customers can help establish customer trust and confidence that their data are being used responsibly. This in turn would make customers more willing to use new products and services.

Along with Zittrain, Yale Law Professor Jack Balkin (2018) has noted the importance of fiduciary duties being a two-way street: It requires “fairness in both directions—fairness to end users, and fairness to businesses, who shouldn’t have new and unpredictable obligations dropped on them by surprise.” Balkin adds that “information fiduciaries should be able to monetize some uses of personal data, and our reasonable expectations of trust must factor that expectation into account. What information fiduciaries may not do is use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm.”

The crux of the fiduciary approach is that the use of the data must benefit the customer. This is different from a no-harm-caused approach because it emphasizes a positive outcome should be the result. In practice, a focus on consumers’ reasonable expectations could mean the fiduciary and legitimate purposes approaches may not be all that different.

BOX 7. **What would violate a fiduciary duty?**

- Using customer data to unfairly manipulate them (e.g., attempt to get people to do something that they would not have done otherwise).
- Using customer data to discriminate against them on impermissible grounds.
- Sharing customer data with third parties without consent.
- Violating the company’s own privacy policies (users’ reasonable expectations mark the limit on data privacy practices).

Source: Dobkin, 2018.



Recommendation 2: Empower Consumers with Modern Digital Rights That Go Beyond Consent

In addition to the legal protections provided by the two new approaches, consumers also should be equipped with digital rights that give them greater control over their personal data trail. For instance, if consumers are denied an account or service, they should have the right to access their data file and correct any inaccuracies. They would want to know why they were denied as it could cause them economic harm, such as denied access to a lower cost loan or a lost job opportunity. GDPR and other recent laws in South Africa and Ghana are equipping people with these rights. Countries like India and the United States are considering legislation and may follow suit.

To empower customers, countries ought to give individuals the following six rights as part of a digital data protection policy:

Right to access personal data. Individuals ought to have the right to access their personal data from a data collector and receive the data in an easy-to-read format. In the European Union, GDPR requires that people be able to see their data,⁸ including which categories of data will be processed and why. In a world of data fluidity, it also requires data controllers to reveal information about the source of their data. There are also time limits within which a data controller must make this information available. In India, the Reserve Bank, like the central banks of many other countries, mandates that credit bureaus provide individuals with one free credit report a year (Zoaib Saleem 2018). In Kenya a few years ago, the money transfer service M-Pesa began allowing customers to download their transaction data in a few easy steps.⁹ Giving people access to their data can make them more aware of what data are being collected and processed and why. It may also help people understand privacy risks and change their behaviors.

Right to update and correct your data. Sometimes inaccurate personal data prevent people from accessing important services. Inaccurate data are not always due to errors. Sometimes they are simply outdated. For instance, someone's tax filing status and level of education may change over time. Modern data protection laws must ensure all systems collecting personal data are equipped to register changes in a person's data and that they do so electronically and with relative ease. GDPR Article 16 allows not only for correction but also the right to complete data that are incomplete.

Right to erase your data. The right to erase one's data can empower customers to prevent their data from spreading. The right to erasure can allow customers to change their mind about a third party holding their data. This would be relevant when customers stop using a service and no longer want a company or service provider to retain their data.

8 General Data Protection Regulation, Art. 15 GDPR, Right of Access by the Data Subject, <https://gdpr-info.eu/art-15-gdpr/>.

9 FAQs, Safaricom, <https://www.safaricom.co.ke/faqs/faq/271>.

Right to port your data. The right to portability goes the furthest in altering the relationship between a data controller and a data subject. GDPR gives people the right to move their data from one data controller to another.¹⁰ It also mandates that controllers transfer data in a format that is usable by another entity, such as a financial services provider. For example, an M-Pesa customer can take his or her payment data to a bank in Kenya to become eligible for a business account or a car loan. Data portability can have a significant impact on how data-based businesses operate. If customers are not happy with the services they receive, they can more easily switch providers by requesting that their data be sent to a competitor. Portability need not be only for switching services. It can also allow individuals to leverage data from one service, such as payments, and use it to become eligible for other services, such as credit or insurance. Expanded creditworthiness can have significant implications for financial inclusion. Many markets are experimenting with unlocking business opportunities and financial inclusion through the responsible flow of data from one entity to another. New infrastructures such as India's Account Aggregators¹¹ or the United Kingdom's Open Banking¹² are building better systems for data sharing across providers.

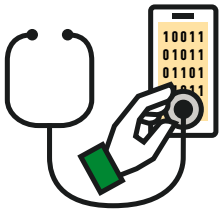
Right to object to information use. Even after a person has granted access to their data, they should have the right to reconsider the decision, either after a period of time or for every new kind of use the data controller requests. The ability to turn off marketing notices from firms who have your data and to have the option to stop one's data from being shared with third parties are important. This is particularly relevant today, when data are increasingly collected for one purpose and deployed for another through third-party applications. GDPR empowers people to object to how their information is used, even after they have provided individual consent. Data controllers will have to abandon all-or-nothing strategies for data use and alert customers on each new kind of processing so they may exercise their choice to opt out.

Rights regarding automated processing. As technologies like AI and machine learning mature, data protection will need to keep up to safeguard customer privacy, including the right to receive an explanation of processing based on AI or machine learning and the right to not be subject to a decision based solely on automated processing.

10 GDPR, Art. 20 GDPR, Right to Data Portability, <https://gdpr-info.eu/art-20-gdpr/>.

11 Account Aggregators are registered entities that enable the sharing of structured financial information with customer consent from one financial firm to another. See Tuli and Co., "Account Aggregators: Financial Information Sharing Framework," <https://www.lexology.com/library/detail.aspx?g=1276b4db-01f7-47b7-8906-a09de711e055>.

12 Open banking in the United Kingdom refers to the specific data-sharing use cases for permitting "third-party intermediaries" to access general information about bank services and prices and allowing third-party providers to access consumers' transactional data based on consumer explicit consent to manage their accounts through a single application. See Sebastian Anthony, "Which Banks Support Open Banking Today?" <https://www.bankrate.com/uk/open-banking/which-banks-support-open-banking-today/>.



Recommendation 3: Enable Fairness in Processing Through Privacy Representatives

Even after a legitimate purposes test or fiduciary requirement is adopted, consumers will need help to navigate a digitally driven world. As businesses adopt data-based models that use increasingly complex forms of AI to make decisions about customers, individuals will lack the ability to monitor and evaluate how decisions about them are being made.

We need privacy representatives, experts who can help consumers by assessing the impact of automated decision-making. This builds on a proposal by Indian privacy lawyer Rahul Matthan (2017) that “learned intermediaries” be appointed to audit for and remedy improper data use. Intermediaries would take the perspective of consumers in evaluating the use of unseen and technically complex algorithms that evaluate people using a wide range of data inputs. Such intermediaries or representatives would focus on the associated risk of unlawful discrimination due to bias built into the design of the algorithm. This may not seem pertinent today for financial inclusion, but it will become increasingly relevant to prevent exclusion as the market includes more and more credit and insurance products that rely on AI and machine learning.

Matthan proposes that intermediaries first review algorithmic queries to assess whether they are being used improperly—for example, whether a lender is seeking an evaluation of risk based on prohibited factors such as gender, race, or caste. Second, intermediaries review algorithmic inputs and outputs to assess whether improper discrimination is occurring. Third, if the second step finds potentially problematic results, intermediaries have access to the algorithm itself, or at least to tools to probe the algorithm, to see if it is compliant. If shortcomings are detected, instead of simply citing the problem, the intermediaries would suggest appropriate remedial measures. The theory is that if the intermediary’s audit results are made public, over time individuals would be drawn to providers whose algorithms are found to be fair and compliant.

In medicine, physicians have been treated as learned intermediaries between pharmaceutical companies and patients, warning patients about potential risks posed by medications. In the data protection context, the role of learned intermediaries could be similar: warning consumers about dangerous data practices or more broadly examining complex privacy notices and industry practices to better educate the public about what they mean and their potential shortcomings.

Intermediaries could be funded by consumers through fees as is the case with financial advisers, they could be offered as a service by nonprofits,¹³ or they could be provided by government agencies as a public service.

In the future, a trusted intermediary may take the form of an app instead of a person—an app that provides guidance about privacy settings, reveals sites that have unsafe privacy practices, and helps delete information providers no longer need.¹⁴

¹³ See, e.g., St. John (2019).

¹⁴ See, e.g., Newton (2019).

CONCLUSION: TRANSITIONING TO A NEW DATA REGIME

THE APPROACHES PROPOSED HERE OF A LEGITIMATE PURPOSES test and a fiduciary duty represent a significant departure from the conventional reliance on individual consent. They put the onus of data protection on the provider instead of the consumer. Further, the adoption of digital rights and privacy representatives would provide individuals with additional guarantees of data protection.

Such progressive approaches will challenge the capacity of many jurisdictions, especially in weaker economies. Their implementation might not happen in one go and their enforcement will take time, yet there is an urgent need to bring such options into policy debates and discussions now. Progress is being made in light of recent advances in technology-based supervision and infrastructure, which make it easier for companies to comply with and for government to enforce data requirements. A key example of this is the recent account-aggregator license created in India. The license allows for data to flow from one financial services company to another once a customer gives consent so that the customer can access new services. It provides customers portability and control of their data.

Protecting data is critical to developing trust and confidence in financial inclusion efforts. Governments considering data protection and privacy legislation are rightly taking a preemptive step to prepare their markets for the opportunities and risks that data-based business models can introduce. However, to be truly effective, they must adopt new approaches that go beyond consumer consent and impose a reasonable burden on providers to act in their customers' interest.

Consent-based models may have been adequate 20 years ago. But as many emerging and developing countries rapidly transition to digital economies, the consent model no longer provides sufficient protections for the technological advances of the 21st century. These countries should be looking to the future and building modern data protections for the kinds of economies they will have in 10 to 20 years. While the data protections outlined here might strain the capacities of many countries, embracing these ideas now will hasten the creation of better data protections that will better enable inclusive growth.



REFERENCES

- ACCC (Australian Competition and Consumer Commission). 2019. “Digital Platforms Inquiry: Final Report.” Canberra: ACCC, June. <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>
- App Annie. 2018. “The Average Smartphone User Accessed Close to 40 Apps per Month in 2017.” App Annie, 2 February. <https://www.appannie.com/en/insights/market-data/apps-used-2017/>
- Bailey, Rishab, Smriti Parsheera, Faiza Rahman, and Renuka Sane. 2018. “Disclosures in Privacy Policies: Does ‘Notice and Consent’ Work?” NIPFP Working Paper No. 246. National Institute of Public Finance and Policy. https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf
- Balkin, Jack M. 2016. “Information Fiduciaries and the First Amendment.” *University of California, Davis, Law Review*, Vol. 49 No. 4. https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf
- Barrett, Lindsey. 2019. “Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries.” *Seattle University Law Review*, 42: 1097. <https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/5/>
- Baur-Yazbeck, Silvia. 2018. “4 Cyber Attacks that Threaten Financial Inclusion.” CGAP blog post, 18 September. <https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion>
- Cakebread, Caroline. 2017. “You’re Not Alone, No One Reads Terms of Service Agreements.” *Business Insider*, 15 November. <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11>
- Dalberg, CGAP, and Future of Finance. 2017. “Privacy on the Line.” Washington, D.C.: Dalberg, CGAP, and Future of Finance. https://www.dalberg.com/system/files/2017-11/Privacy%20On%20The%20Line%20Final%20161117_1.pdf
- Data Protection Committee. N.d. “A Free and Fair Digital Economy Protecting Privacy, Empowering Indians.” New Delhi: Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. 2018. “The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution.” Washington, D.C.: World Bank.
- Dobkin, Ariel. 2018. “Information Fiduciaries in Practice: Data Privacy and User Expectations.” *Berkeley Technology Law Journal*, Vol 33:1. http://btlj.org/data/articles2018/vol33/33_1/Dobkin_Web.pdf
- Edwards, John. 2019. “Click to Consent? Not Good Enough Anymore.” Privacy Commissioner blog post, 2 September. <https://privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/>
- GSMA 2019. “The Mobile Economy 2019.” London: GSMA. <https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download>
- ICO (Information Commissioner’s Office). 2018. “Lawful Basis for Processing: Legitimate Interests.” Wilmslow: ICO, March. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/>
- — —. 2019. “Guide to the General Data Protection Regulation.” Wilmslow: ICO, May. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>
- ID4D: World Bank Group. Accessed 20 November 2019. <https://id4d.worldbank.org/global-dataset>.
- Khan, Lina, and David Pozen. 2019. “A Skeptical View of Information Fiduciaries.” Columbia Public Law Research Paper No. 14–622. New York: Columbia University Law School. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341661
- Loucks, Jeff. 2018. “First Control, Then Consent.” Deloitte, Perspective, 6 September. <https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/personal-data-privacy-regulations-and-consent-of-consumers.html>

- Madrigal, Alexis C. 2012. "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days." *The Atlantic*, 1 March. <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>
- Matthan, Rahul. 2017. "Beyond Consent: A New Paradigm for Data Protection." Discussion Document 2017-03. Bangalore: Takshashila Institution. <https://takshashila.org.in/discussion-document-beyond-consent-new-paradigm-data-protection/>
- McLean, Rob. 2019. "A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts." *CNN Business*, 30 July. <https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html>
- Newton, Casey. 2019. "Jumbo Is a Powerful Privacy Assistant for iOS That Cleans up Your Social Profiles." *TheVerge.com* blog post, 9 April. <https://www.theverge.com/2019/4/9/18300775/jumbo-privacy-app-twitter-facebook>
- Ng, Alfred. 2019. "Microsoft Wants a US Privacy Law That Puts the Burden on Tech Companies." *CNET* blog post, 20 May. <https://www.cnet.com/news/microsoft-wants-a-us-privacy-law-that-puts-the-burden-on-tech-companies>
- Ohm, Paul. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review*, Vol. 57, last revised 22 February 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006
- Pichai, Sundar. 2019. "Google's Sundar Pichai: Privacy Should Not Be a Luxury Good." *New York Times*, Opinion, 7 May. <https://nyti.ms/2POJzWI>
- Regalado, Antonio. 2019. "Facebook Is Funding Brain Experiments to Create a Device That Reads Your Mind." *MIT Technology Review*, 30 July. https://www.technologyreview.com/s/614034/facebook-is-funding-brain-experiments-to-create-a-device-that-reads-your-mind/?utm_source=nextdraft&utm_medium=email
- Sathe, Gopal. 2019. "How Sai Baba Was Made to Spy on Your Phone for Credit Ratings." *HuffPost* blog post, 7 August. https://www.huffingtonpost.in/entry/fintech-apps-privacy-snooping-credit-vidya_in_5d1cbc34e4b082e55373370a
- St. John, Allen. 2019. "Consumer Reports Launches New Digital Lab." *Consumer Reports*, 6 June. <https://www.consumerreports.org/privacy/consumer-reports-launches-digital-lab/>
- Valentino-Devries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik. 2018. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *New York Times*, 10 December. <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?action=click&module=Top%20Stories&pgtype=Homepage>
- Warzel, Charlie. 2019. "FaceApp Shows We Care About Privacy but Don't Understand It." *New York Times*, Opinion 18 July. <https://www.nytimes.com/2019/07/18/opinion/faceapp-privacy.html>
- Wood, Alexandra, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, James Honaker, Kobbi Nissim, David R. O'Brien, Thomas Steinke, and Salil Vadhan. 2018. "Differential Privacy: A Primer for a Non-technical Audience." *Jet Law*, 14 February. https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_new.pdf
- Zittrain, Johnathan. 2018. "How to Exercise the Power You Didn't Ask for." *Harvard Business Review*, 29 October. <https://blogs.harvard.edu/jzwrites/2018/10/29/how-to-exercise-the-power-you-didnt-ask-for/>
- Zoib Saleem, Shaikh. 2018. "You Can Get 4 Free Credit Reports Each Year." *Livemint.com*, 21 May. <https://www.livemint.com/Money/HSMi5PkB86aek34QLParjN/You-can-get-4-free-credit-reports-each-year.html>

