JULY 2020

CHARTING A WAY FORWARD

Communicating About Privacy: Towards People-Centered and Accountable Design

Erin Egan

VICE PRESIDENT AND
CHIEF PRIVACY OFFICER, PUBLIC POLICY

FACEBOOK

Table of Contents

Introduction 01

There is an active and ongoing global discussion about how, when, and whether companies should use data about people, how people can be empowered to make meaningful decisions about that data, and what laws and regulations should apply.

Grounding this discussion is the importance of people's basic rights to be informed about how their information is collected and processed. Without this crucial information, people cannot make choices about what digital services to use and how to engage with controls offered by companies for limiting and exercising their rights.

And yet, there is a fundamental paradox: people need to be informed, but it doesn't help just to give people more information. People have to be *meaningfully* informed, in a way that empowers them to make choices about how they participate online and share their data. That means: notice has to be relevant to their needs and expectations, understandable, accessible, and simple. Despite this, today people are currently informed through documents and websites that might satisfy the law, but can be hard to find, filled with legalese, or simply confusing. Privacy policies are often written by lawyers for other lawyers.[1] According to one study, it would take the average person 40 minutes a day to read the privacy policies for the services they use.[2] And even when people do read these policies, it can be hard for people to connect them with their activities and experiences online.

Over the past few decades, many companies, including Facebook, have worked to make privacy notices more user-friendly by adopting practices like layered privacy policies, just-in-time notices, and in-context notifications.[3] Regulators have also given guidance on good notification practices,[4] including how to design notices for children,[5] how to design "clear and conspicuous"[6] notices, and how to provide information in a “concise, transparent, intelligible, easily accessible [form] and using clear and plain language.”[7] Still, these practices remain inconsistently adopted, if at all. And there isn’t clarity on which practices best convey information to people.

In short, the current practices for informing people about how companies use their data, and the laws setting out transparency requirements, may be insufficient to provide meaningful notice to people.

This leads to two observations: First, privacy policies cannot be the only ways that companies communicate with people about their information. Second, rather than simply meeting minimum legal standards, companies need to find new ways to both inform and empower people to make privacy choices that are meaningful for them.

As a starting point, it is important to focus on people, how they understand privacy information, and how they interact with different privacy notifications like layered or contextual notices. Effective communication about privacy also means recognizing—and designing for—the diversity of people who use digital services and how people understand and interact with evolving technologies like connected devices and artificial intelligence. Only by putting people at the center can we develop better approaches to communicating with them.

At Facebook, we embrace our responsibility to help people become informed—and stay informed—about how and when their data is collected, shared, and used. As we look to improve our own approaches, we want to work with policymakers, academics, and other companies to find new solutions. This paper is intended to be a starting point for that conversation.

With this in mind, in the first part of this paper, we explore some of the tensions inherent in existing privacy notice design and new technology. In the second part, we identify three key questions for further consideration and suggest potential paths forward:

01 How can organizations, regulators, and other stakeholders collaborate on a people-centered approach to the development, testing, and evolution of new ways to communicate about privacy that meet the diverse needs of a global community?

02 How can laws and regulation better foster the use of people-centered design practices for privacy communication?

03 How can regulators hold organizations accountable while also enabling them to fully embrace people-centered design for privacy communication?

We hope to be part of the process that develops new ideas, which in turn are refined by multi-stakeholder groups and incorporated into future regulatory frameworks. In Appendix A, we set out a series of questions on which we will seek input in the coming months.

The Inherent Tensions with Communicating about Privacy

02

In today's interconnected world, many companies provide services to a global and diverse set of people. In order for companies to meaningfully inform these people about how their information is collected and processed, companies must go beyond traditional approaches to compliance and account for how people process information in different contexts, as well as their distinct goals and preferences. Going forward, even the best policy solutions will not only have to be tailored to different industries and different use cases, but also to different groups of people.

A. PRIORITIES OF TRANSPARENCY

Meaningful transparency—that is, the concept of informing people what information about them is held and how it is processed—is a foundational aspect of privacy law and regulation, not only because it empowers people to make choices about their information, but also because it creates pressure on organizations to handle data responsibly.[8] In the context of privacy, the concept of transparency was first codified decades ago in the Organisation for Economic Co-operation and Development ("OECD")'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which included obligations around openness and guidelines for enabling an individual to participate in governance of his or her data.[9] Since then, transparency has been codified in other foundational privacy frameworks like the Council of Europe's Convention for the protection of individuals with regard to the processing of personal data ("Convention 108"),[10] Europe's Data Protection Directive,[11] and later, the General Data Protection Regulation ("GDPR"), which reiterated the core principle of transparency and required information to be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language.[12]

Over time, experts have identified a range of principles and standards that can help organizations effectively communicate about privacy, including:

> **Comprehensiveness.** Privacy notifications should be complete enough to provide a comprehensive reflection of an organization's data practices.[13]
>
> **Comprehensibility.** Notifications should be written in a way that prioritizes the most important information and is easy for people to understand.[14]
>
> **Prominence.** Notifications should be presented in a way that is clear and conspicuous, or that attracts people's attention.[15]
>
> **Standardized.** Information should be presented in a way that is consistent across products and services, to make it easier for people to evaluate information and make choices in different contexts.[16]
>
> **Contextual.** Notifications should be designed in a way that is consistent with their environment to make them more intuitive and to enable quicker and more effective decision-making.[17]

Each of these principles is important, but there are also critical tensions between them, and favoring one sometimes means compromising others. To make progress on meaningful transparency, it is important to explore these tensions and identify practices that can mitigate them.

B. DESIGN TENSIONS

The design of privacy notices can affect how people understand their privacy choices and feel empowered to act on them.

1. Comprehensiveness vs. Comprehensibility

Privacy laws generally require companies to inform people about their information practices, including: what personal information they collect, how it is used, and with whom it is shared. Some laws go further and require notice of things like: the use of certain types of automated decision-making, the specific provision of law (or "legal basis") that authorizes each processing of data, and whether personal data will be transferred to another country.[18]

And yet, because additional transparency also means lengthier and more complex privacy disclosures, there is an inherent tension between the comprehensiveness of information and the likelihood that people will read and understand it.

Limiting the length and improving the readability of privacy notices can increase comprehension, but doing so can sacrifice important or otherwise legally required details and disclosures. The noted privacy scholar Helen Nissenbaum describes this dilemma as the "transparency paradox":

> If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference . . . An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance.[19]

One solution to the transparency paradox is to better align organizations' practices with people's reasonable expectations, a concept Nissenbaum describes as "contextual integrity." But in improving communication to people, more work is required to develop the right balance between making disclosures comprehensive and making them understandable.

2. Prominence vs. Click Fatigue

Privacy notices are an important tool for keeping people informed of how and when their data is used and collected. However, more notices are not necessarily better. For example, multiple pop-ups and other prominent notices will likely be noticed but can interrupt people's product or service experience. As with the transparency paradox, however, there is a tension in notice design: the more notifications you show to someone, the less likely that person is to apprehend or absorb any one particular notice and make informed choices about their data. The more notices that companies display, the greater the chance of creating "click fatigue," whereby people skip over the words and click through to continue using the service.[20] Similar-looking notices can exacerbate this problem by training people to mistakenly anticipate their content—a concern some have raised about the proliferation of "cookie banners" on most websites in Europe.[21]

However, placing notices too far from a user's immediate experience can also make that information harder to find and less likely to be seen. As a result, people may ignore these notices that are legally sufficient but deficient in terms of accessibility, and thus do not take in important privacy information.

In view of these tensions, the people who design notices face a complex challenge. They must convey the most salient information in the interface, while ensuring less-salient information is still accessible. They must also provide the right number of notices at the right time so that people will be meaningfully informed.

3. Design Standardization vs. Design Adaptability

Other design decisions that affect people's attention to (and comprehension of) what they read include aesthetic factors like: the placement of notices, the size and color of fonts, and the headings.[22] These factors may even influence people's decisions about their data.[23] This may be why some privacy frameworks and legislation require or encourage uniform design elements to convey privacy information, *e.g.*, specific language[24] or standardized icons.[25] Standardization can help people understand what to expect and make more meaningful comparisons across different apps and services.

However, standardization has its trade-offs. Unlike, for example, the basic composition of food products that are catalogued in a standardized nutritional label, the data practices of different organizations providing different services are far from uniform. Any standardized notice method risks omitting nuances critical to meaningful understanding. And excessive standardization could lead to people ignoring notifications altogether.

Additionally, companies today make products and services for people with a range of educational backgrounds, language skills, physical abilities, technological and literacy levels, and individual preferences about how they receive information. It can be challenging to make important information accessible and comprehensible to everyone, and standardized notification requirements can fail to meet the diverse needs of different groups of people.

For example, experts have suggested that text-based disclosures may not be an effective way of communicating with communities that are new to the Internet, that don't have a consistent level of literacy across the population, or that have a diversity of languages.[26] The use of video and animation may partially address these concerns, but it might not be accessible to the people without a powerful device and a strong Internet connection, which may not be available or broadly used in many parts of the world. More work is needed to develop strong practices for communicating privacy information to people around the world, each of whom approaches this issue with different preferences and needs.

C. NEW TECHNOLOGIES AND INTERFACES

Newer technologies like artificial intelligence, connected devices, and virtual and augmented reality promise improvements in the way people interact with technology and with each other. These technologies also present opportunities for communicating with people about privacy and empowering them in new ways.

At the same time, because these technologies weren't envisioned when many of today's practices around transparency were adopted, they raise new questions about how to apply conventional approaches to new contexts.

1. Artificial Intelligence

The term "artificial intelligence" (or "AI") doesn't have a universal definition, but it generally refers to machine-based systems that can predict, recommend, decide, perceive, interpret, or learn at or beyond the ability of humans. Some common tasks performed with the help of AI include: identifying contents of photographs, automatically translating between languages, and sorting and recommending information.

Because of its underlying complexity, AI challenges the imperative to make data processing more transparent. With AI, transparency is tied to explainability because in most cases simply providing information about an algorithm does not, on its own, provide meaningful transparency.

According to the OECD, transparency and explainability in AI systems serve four major goals:

- Fostering a **general understanding** of AI systems.
- Making stakeholders **aware of their interactions with AI systems**, including in the workplace.
- Enabling those affected by an AI system to **understand the outcome**.
- Enabling those adversely affected by an AI system to **challenge its outcome** based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.[27]

A significant challenge for achieving meaningful transparency in machine learning models (one form of AI) is that some models are highly complex, relying on thousands or even millions of signals to accomplish their goals. By their nature, machine learning models are designed to dynamically evaluate a large number of factors toward a predetermined goal, so explaining how they operate in an intuitive and actionable way often isn't straightforward.

For this reason, researchers are exploring new methods of explaining the material aspects of a machine learning model's functionality in a way that is accessible to people and informs their own decision-making.[28] One view of transparency in the context of machine learning generally focuses on surfacing two aspects: (1) the factors that are used as inputs to the model, and (2) the outputs of a model under a range of circumstances. According to this view, even if the internal workings of a model are not readily explainable, sharing what inputs the model considers and how that analysis can result in different outcomes can improve transparency.[29] Additional views of transparency look at explainability in context, focusing on the justification of the use, intent and goals of the AI system, and identifying different types of explanations.[30]

Finally, meaningful transparency in the context of AI doesn't just mean helping people understand AI decision-making processes. It also means considering: At what point is it most helpful or appropriate to provide notice? At the time data is collected? When that data is used to train models? When those models are used to make a prediction or to shape a user's experience? Answering these questions is key to providing information to people in ways that are meaningful for them.

2. Connected Devices and Virtual and Augmented Reality

Other evolving technologies like in-home connected devices (*e.g.*, speakers and video calling), Virtual Reality ("VR"), and Augmented Reality ("AR")[31] pose additional questions and present new opportunities for privacy notification design.

For instance, typical practices for transparency today—things like privacy policies or in-product notices—may not be meaningful or even possible in the context of in-home devices that do not have interfaces to communicate information. In addition, different people within the same household may share the same devices. Therefore, communicating about data collection practices and choices—often without the use of interfaces—requires special consideration.

Also, meaningful transparency in the context of AR and VR must acknowledge that data collection and uses in these contexts may be different from traditional technologies. In order to function, AR and VR systems process things like a person's physical location in a space and information about people's physical characteristics, some of which people might consider "particularly private."[32] For example, advanced VR systems may use technology to measure the movement of people's eyes in order to provide a higher-resolution, more immersive experience.

At the same time, these new technologies provide opportunities for creative solutions for privacy notifications. VR and AR products feature a range of user interfaces, some fully interactive and immersive, such as VR headsets, and others readily incorporated into everyday activities, such as AR eyeglasses. These interfaces introduce additional moments for providing privacy notifications and often must do so in creative ways because traditional ways of interacting with digital information, such as clicking on hyperlinks, may not be possible.

Overall, companies using these new technologies need to use data in new ways to provide innovative services that people are asking for—but companies must do so in a way that minimizes the privacy impact of their data practices while communicating those practices clearly. Designing new technologies requires a nuanced understanding of both the benefits they bring and the unintended consequences to avoid.

Charting a Path Forward 03

While there are no easy or obvious solutions to the challenge of transparency, there are exciting new paths forward. One path highlighted here is to consider privacy notifications as dynamic design challenges, and not just as formalistic compliance obligations.

In particular, it is worth considering the potential of adapting the same design tools and methodologies that technology companies rely on to develop their core products and services, sometimes called “human-centric design” or “people-centered design.” This is an approach that focuses on the needs, concerns, and preferences of people at every step in the product design process, from ideation to iteration, launch and improvement. If organizations consistently applied that same user-focused and iterative design process to designing privacy-related notices and controls, the results could very well be transformative.

This Part sets out three key questions—and suggests potential answers—that are central to determining whether and how to leverage better design solutions to enhance privacy communications with people:

01 How can organizations, regulators, and other stakeholders collaborate on a people-centered approach to the development, testing, and evolution of new ways to communicate about privacy that meet the diverse needs of a global community?

02 How can laws and regulation support the potential of using people-centered design practices for privacy communication?

03 How can regulators hold organizations accountable while also enabling them to fully embrace people-centered design for privacy communication?

QUESTION 1

How can organizations, regulators, policymakers, and experts collaborate on a people-centered approach to the development, testing, and evolution of new transparency mechanisms that meet the diverse needs of a global community?

As the first section of this paper describes, there are a range of priorities and considerations that anyone designing privacy notifications must take into account. This is true both as a general matter, and when it comes to meeting the needs of diverse populations—people with differing cultural norms, differing levels of access to technology, or who may have preferences or specific needs around how they receive information.

Transparency efforts by organizations, as well as the policy frameworks that underlie them, must be built to anticipate and meet varying needs. There are no easy answers, nor has anyone "solved" the problem of how to design transparency to address these needs. When it comes to both developing effective design patterns and policies governing transparency, collaboration is needed to more clearly identify the challenges and create successful solutions.

One potential path toward this goal is to explore policy co-creation strategies, which are ways of collaborating that enable direct, constructive engagement between regulators, policymakers, companies, and other experts. Policy co-creation offers some benefits over traditional processes:

- First, it allows regulators to work with industry and experts to better understand the products and technologies involved, identify concerns, and establish clear, upfront goals for privacy notices.
- Second, policies and tools can be prototyped and tested for viability and effectiveness before they are fully implemented. This is especially helpful for small and medium-sized businesses, which have limited resources to invest in improving their privacy notifications.
- Finally, both companies and regulators can achieve better clarity about the outcomes they want to achieve.

Perhaps the most well-known method for policy co-creation is a "regulatory sandbox." Sandboxes are policy innovation labs that are also spaces for ideation, iteration, and experimentation. In these sandboxes, and within strict parameters, regulators can introduce temporary regulatory flexibility on specific legal requirements for specific companies. Regulators and companies can then work together to test new approaches to particular challenges (such as transparency) within a contained regulatory environment. In this way, ideas can be explored in a collaborative but responsible fashion.[33] The goal of sandboxes is not to absolve companies of responsibility over their data practices; rather, it is to provide a collaborative mechanism for understanding the goals and effects of regulation and designing approaches that appropriately address them.

Sandboxes have been used in other sectors, like the financial sector, for years. At least two data protection authorities are now using them to tackle pressing regulatory challenges.[34] Policy co-creation strategies require significant resources from regulators and the level of interest to date suggests that regulators view the resource commitment valuable in the long term.

In 2017, Facebook launched "Trust, Transparency and Control Labs," or TTC Labs, to bring together those who work on privacy in government, industry, academia, the design community, and civil society to devise solutions for improving transparency and control across digital services. In Singapore, TTC Labs worked with the Infocomm Media Development Authority to create the "Facebook Accelerator", a startup programme that included a regulatory sandbox. This initiative enabled startups to find new ways to increase the reach of their businesses while maintaining people' s trust and giving them control over their data. Through intensive collaboration efforts like Design Jams,[35] startups in the Accelerator received ongoing compliance guidance and support from regulators, and regulators could better understand startups' business models and design approaches.[36]

These Design Jams identified several new design prototypes that are explored in more depth in Appendix C to this paper and in the TTC Labs report titled, "People-Centric Approaches to Notice, Consent and Disclosure."[37]

QUESTION 2

How can regulation better enable the use of people-centered design practices for privacy communication?

Effective laws and regulation can create the conditions for businesses to develop people-centered design practices. However, many current privacy laws end up incentivizing traditional, long-form—and historically ineffective—forms of notice.

While there are examples of regulators providing examples of "good practices" in this space,[38] as a general rule regulators are understandably hesitant to pre-approve a new or untested method for a privacy notice. This leaves companies with uncertainty about whether a particular approach will be acceptable to regulators. Even with extensive testing, there are no guarantees that new designs will perform as intended or expected when they are rolled out to real people. And even if a new notice proves to be more effective, regulators may determine the design still does not meet their expectations.

In addition, the mere fact that a company evolves its privacy notice design over time could be perceived by regulators as evidence that prior versions were insufficient and, therefore, potentially unlawful. Keeping people informed about their data requires experimentation, but that carries the risk of regulators misconstruing these activities as admissions that prior practices were ineffective, asking, in effect: if it wasn't broken, why fix it?

One way forward is for regulators, at a minimum, to avoid or remove strict, one-size-fits-all design requirements. But beyond that, it will be important to consider ways to expect and encourage more people-centric design practices, while ensuring that bad actors aren't abusing any flexibility to intentionally game the system using "dark patterns" or other design tricks.[39] For example, regulations could create a "safe harbor" from enforcement for companies that adhere to specific design principles, or that demonstrate "design process accountability," discussed further below.

QUESTION 3

How can regulators hold organizations accountable while also enabling them to fully embrace people-centered design for privacy communication?

If collaborative processes seem like a good way forward and current legal standards could be reconsidered, the question remains: what standards *should* companies be held to for providing meaningful notices and controls?

1. Co-created Standards

In line with policy co-creation, discussed above, regulators, industry and other stakeholders could focus on prototyping context-specific, data-specific or industry-specific standards.

For example, regulators could establish robust processes and parameters for developing and sharing these practices. To start, they could focus on a particular sector, a particular data use, or a particular objective (*e.g,*. obtaining consent). Industry members could then define the standards in that area, recognizing the need for variation among organizations, and a regulatory body could require those best practices or allow companies to voluntarily comply and demonstrate compliance to a certifying third party.

This co-creation approach would help improve privacy notification practices because, in addition to organizations using their own judgment about how to approach communicating with people, regulator-approved and enforceable best practices could be established where none currently exist.

2. Design Process Accountability

Another idea for regulators could be to regulate the process for making privacy design decisions, not the outcome of those processes.

In the corporate world, this focus is known as "accountability," and often covers things like corporate responsibility, governance, and stewardship. In short, accountability can be described as: "a framework that operationalizes and translates principles-based laws into effective internal policies, procedures, controls and governance programs, with external guidance from regulators and advisers."[40]

In the data protection sphere, accountability requires companies to demonstrate, among other things:

- **Leadership and oversight**, by establishing a privacy management program and ensuring appropriate reporting;
- **Implementation** and operationalization of applicable program requirements; and
- **Monitoring and verification** of ongoing internal compliance.[41]

Accountability looks different for every company—depending on the applicable legal requirements, internal processes and goals, and the specific data and use-cases involved—but it meets a common, accepted standard.

In the context of transparency, "design process accountability" could require demonstrating similar concepts as in data protection accountability. Rather than expecting companies to implement a specific design set out in the law, companies could instead be expected to implement and be able to demonstrate a design *process* for privacy-related notices and controls that would meet certain established goals. In this way, organizations could work to improve their established practices, while also achieving the fundamental purpose of transparency, without being penalized for attempting to improve the status quo.

And since there are no universal standards for privacy notifications, companies could develop and implement their own design principles, such as offering people accessible, easy-to-use controls over their data, evaluating and considering alternate designs, and engaging in user research where appropriate.

As with all accountability programs, for design process accountability to work it has to take into account a company's size, the different types of services it offers, and the relative risks involved with the type of data it collects and uses.

Conclusion 04

Facebook recognizes the responsibility we have to make sure that people are informed about the data that we collect, use, and share.

That's why we support globally consistent comprehensive privacy laws and regulations that, among other things, establish people's basic rights to be informed about how their information is collected, used, and shared, and impose obligations for organizations to do the same, including the obligation to build internal processes that maintain accountability.

As improvements to technology challenge historic approaches to effective communications with people about privacy, companies and regulators need to keep up with changing times.

To serve the needs of a global community, on both the platforms that exist now and those that are yet to be developed, we want to work with regulators, companies, and other interested third parties to develop new ways of informing people about their data, empowering them to make meaningful choices, and holding ourselves accountable.

While we don't have all the answers, there are many opportunities for businesses and regulators to embrace modern design methods, new opportunities for better collaboration, and innovative ways to hold organizations accountable.

In the coming months, we will host conversations with regulators, civil society, academics, and other companies around the world to dive into the questions raised in this paper and elaborated on more fully in Appendix A.

APPENDIX A

Additional Questions to Consider

How can organizations, regulators, policymakers, and experts collaborate on a people-centered approach to the development, testing, and evolution of new transparency mechanisms that meet the diverse needs of a global community?

- How could these processes be adopted and experimented with in the context of privacy? Are there any existing examples?
- Are there examples of policy co-creation processes used in other contexts or industries that should be considered?
- Who should be included in the process of policy co-creation and what should their roles be?

How can regulation better enable the use of people-centered design practices for privacy communication?

- Do existing regulations pose challenges to the use of people-centered design practices?
- How can regulations create clear obligations while enabling diverging approaches to transparency and design based on context and intended audiences?
- How can regulations encourage organizations—particularly small organizations without substantial resources—to engage in people-centered iterative design processes to improve transparency and control?

How can regulators hold organizations accountable while also enabling them to fully embrace people-centered design for privacy communication?

- What is the role of enforceable best practices and standards in a regulatory framework that prioritizes people-centered design?
- Would targeted industry- or context-specific best practices be appropriate in certain circumstances?
- What elements would enforceable regulation of “design process accountability” regulation include?

APPENDIX B

TTC Labs

TTC Labs (ttclabs.net) is a cross-industry effort to create innovative design solutions that put people in control of their privacy. Initiated and supported by Facebook, and built on collaboration and co-creation, the movement has grown to involve over 250 stakeholders, including major global businesses, startups, civic organizations, and academic institutions.

TTC Labs uses design thinking-methods leveraged by designers to make technology usable and people's lives simpler, and to create new tools to inform people about their data and choices in ways that are intuitive and accessible.

To create these new tools, TTC Labs runs "Design Jams," interactive one-day workshops on issues of trust, transparency and control in the digital space. They bring together diverse stakeholders with different viewpoints. These stakeholders share ideas, develop new perspectives and create digital prototypes that bring their ideas to life.

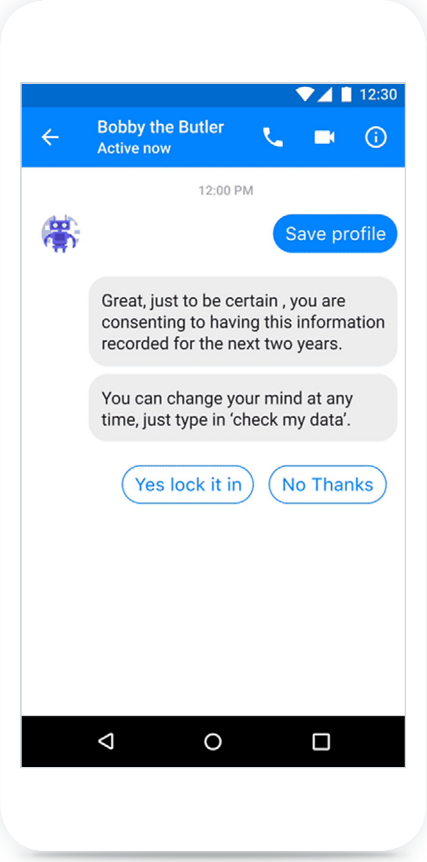
Working together, they co-design and test promising design models in a way that helps inform future policy-making. To date, TTC Labs has run 28 Design Jams in 11 cities around the world, and it's only the beginning. These Design Jams have explored designs for a range of scenarios, from the use of biometric data and AI, to designing for safety and age verification for children.

Design Jams outputs have real-world impact: new design templates are compiled on the TTC Labs website, available for everyone to use. In addition, the website also offers an open-source toolkit that anyone can use to run a Design Jam.

APPENDIX C

Design Examples

The Design Jams held as part of the Facebook Accelerator program with the Infocomm Media Development Authority in Singapore produced several promising new design prototypes. Several of them are shown below, along with examples of how Facebook has implemented similar approaches in its privacy controls over time.

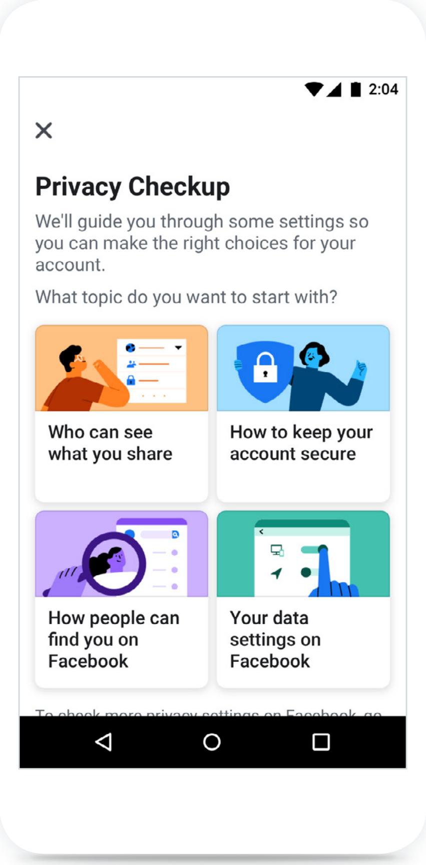


Great, just to be certain , you are consenting to having this information recorded for the next two years.

You can change your mind at any time, just type in 'check my data'.

Proactive check-in

An unprompted check-in happens when the system randomly provides information or asks for your review of choices, rather than passively waiting for a person to seek out and engage with controls. This is a helpful mechanism for keeping people consistently informed about their data decisions. The proactive check-in mechanism also helps technology teams to build trust with people over time by actively encouraging a dialogue about data management.



Privacy Checkup

We'll guide you through some settings so you can make the right choices for your account.

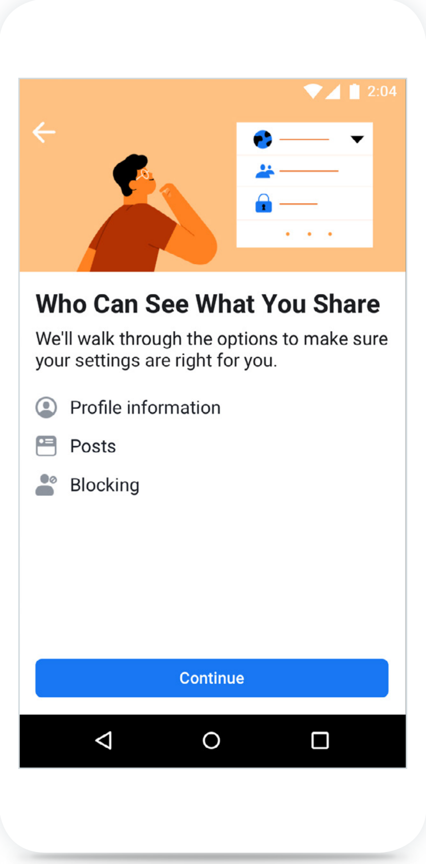
What topic do you want to start with?

- Who can see what you share
- How to keep your account secure
- How people can find you on Facebook
- Your data settings on Facebook

To check more privacy settings on Facebook, go

FACEBOOK'S APPROACH

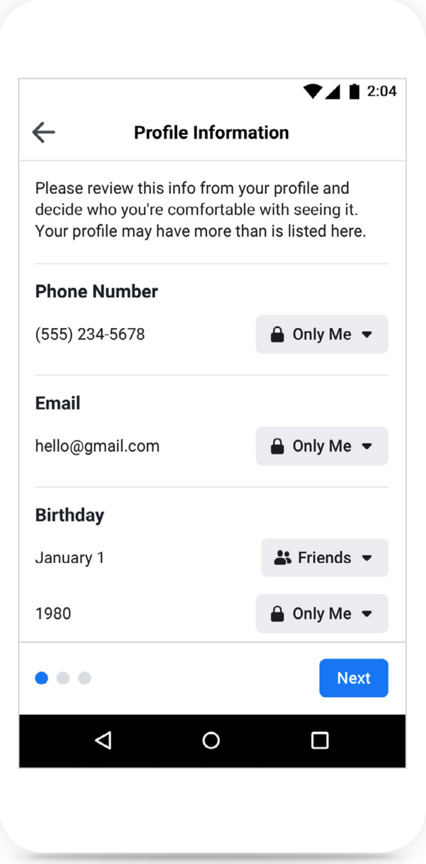
Facebook has implemented—and iterated over time—a proactive check-in in the form of the Privacy Checkup[42] tool. We recently updated Privacy Checkup and sent prompts to nearly 2 billion people, encouraging them to revisit their privacy choices.[43] The process asks people to review four important aspects of their privacy on Facebook: the audience who will see their Facebook posts, how to keep their accounts secure, how people can find them on Facebook and the data they share with apps they've logged into with Facebook.



Who Can See What You Share

We'll walk through the options to make sure your settings are right for you.

- Profile information
- Posts
- Blocking



Profile Information

Please review this info from your profile and decide who you're comfortable with seeing it. Your profile may have more than is listed here.

Phone Number

(555) 234-5678 — Only Me

Email

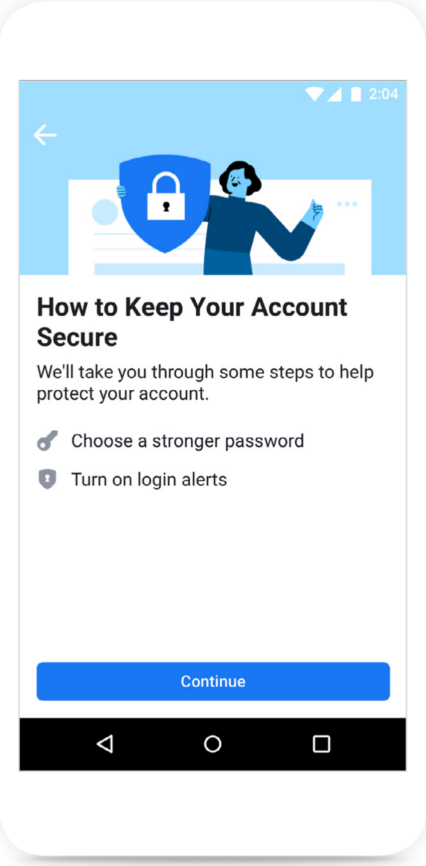
hello@gmail.com — Only Me

Birthday

January 1 — Friends

1980 — Only Me

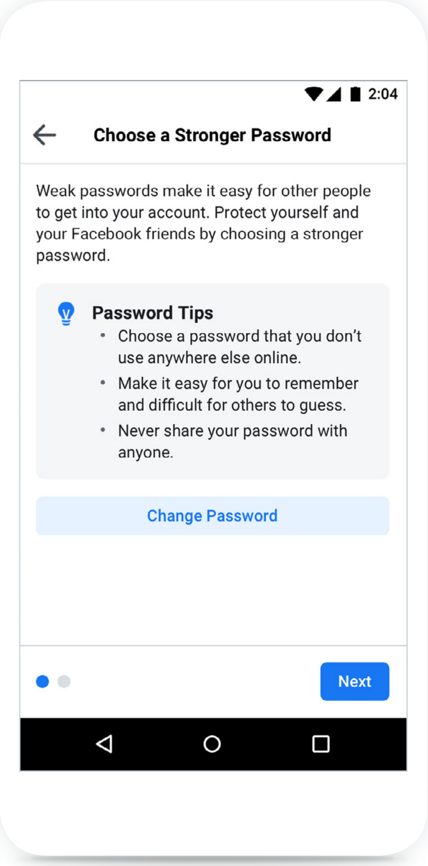
Who Can See What You Share will help you review who can see your profile information, like your phone number and email address, as well as your posts.



How to Keep Your Account Secure

We'll take you through some steps to help protect your account.

- Choose a stronger password
- Turn on login alerts



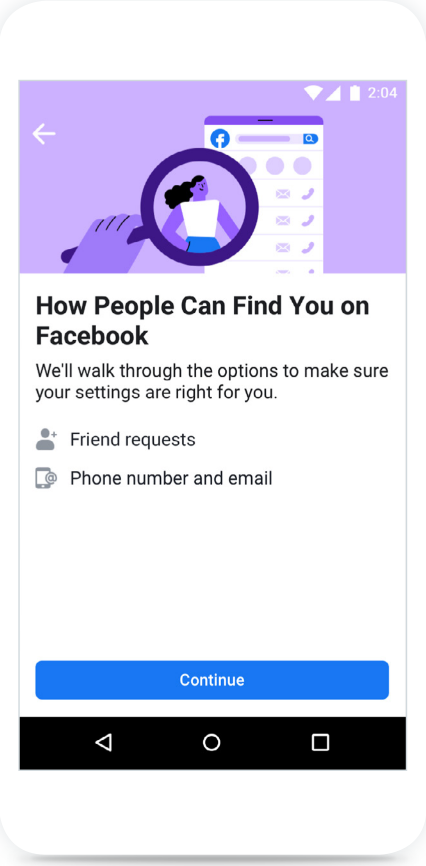
Choose a Stronger Password

Weak passwords make it easy for other people to get into your account. Protect yourself and your Facebook friends by choosing a stronger password.

Password Tips

- Choose a password that you don't use anywhere else online.
- Make it easy for you to remember and difficult for others to guess.
- Never share your password with anyone.

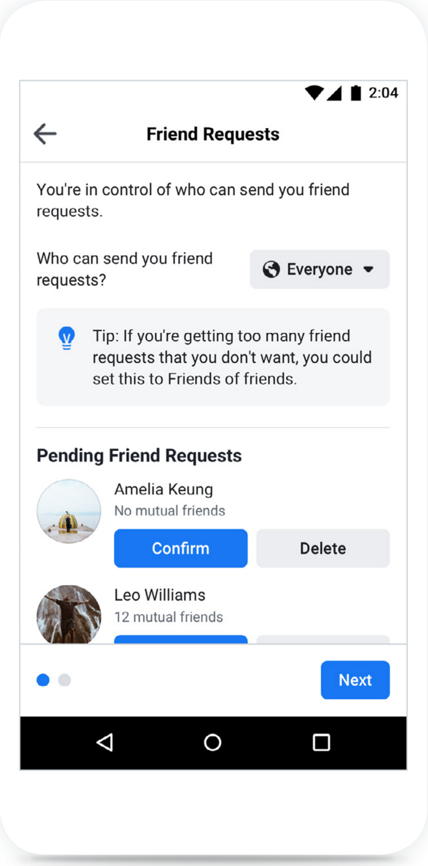
How to Keep Your Account Secure will help you strengthen your account security by setting a stronger password and turning on login alerts.



How People Can Find You on Facebook

We'll walk through the options to make sure your settings are right for you.

- Friend requests
- Phone number and email



Friend Requests

You're in control of who can send you friend requests.

Who can send you friend requests? Everyone

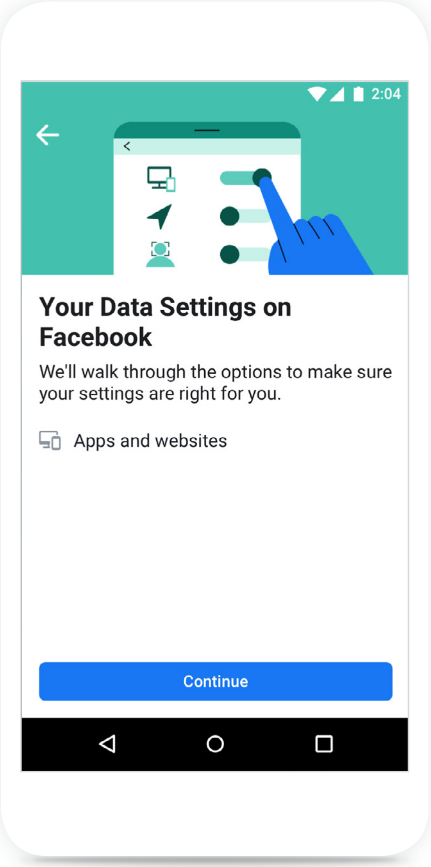
Tip: If you're getting too many friend requests that you don't want, you could set this to Friends of friends.

Pending Friend Requests

Amelia Keung
No mutual friends

Leo Williams
12 mutual friends

How People Can Find You on Facebook will let you review ways in which people can look you up on Facebook and who can send you friend requests.

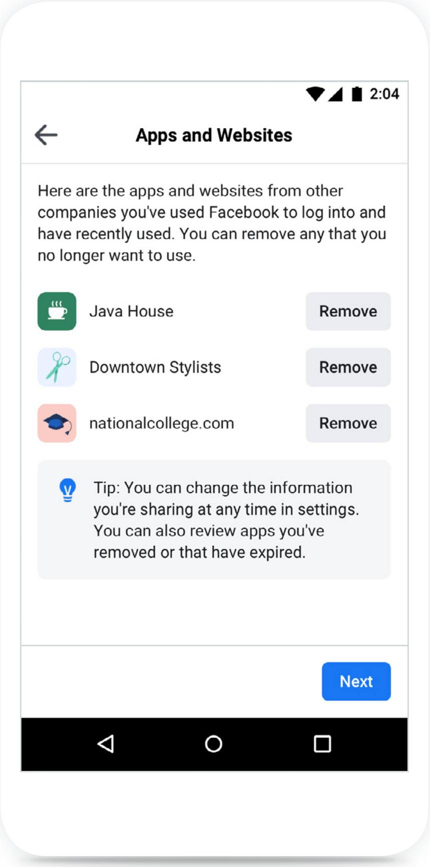


2:04

Your Data Settings on Facebook

We'll walk through the options to make sure your settings are right for you.

Apps and websites



2:04

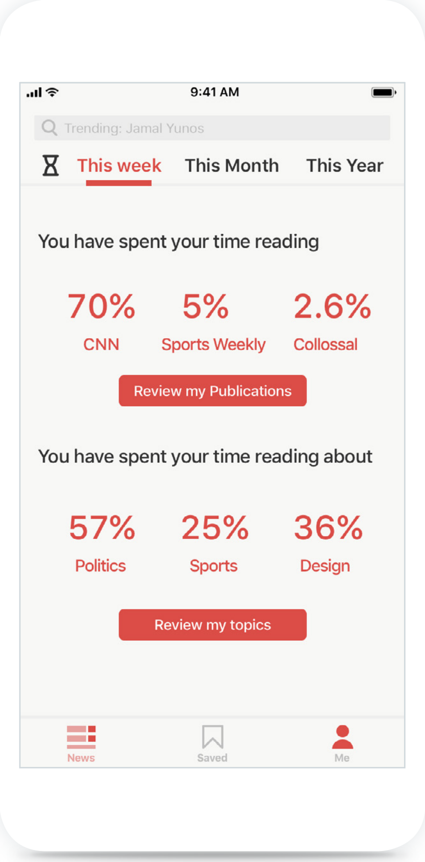
Apps and Websites

Here are the apps and websites from other companies you've used Facebook to log into and have recently used. You can remove any that you no longer want to use.

Java House	Remove
Downtown Stylists	Remove
nationalcollege.com	Remove

Tip: You can change the information you're sharing at any time in settings. You can also review apps you've removed or that have expired.

Your Data Settings on Facebook will let you review the information you share with apps you've logged into with Facebook. You can also remove the apps you no longer use.



9:41 AM

Trending: Jamal Yunos

This week | This Month | This Year

You have spent your time reading

70%	5%	2.6%
CNN	Sports Weekly	Collossal

Review my Publications

You have spent your time reading about

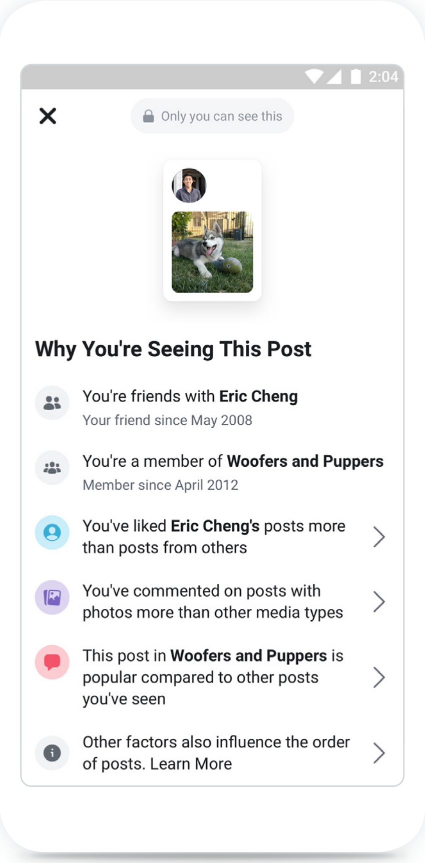
57%	25%	36%
Politics	Sports	Design

Review my topics

Simple Summaries

Simple, clear summaries can be effective at conveying information to people about how they use or engage on a particular service over time. This is especially relevant if a person's activities on a platform influence their future platform experience. Unlike technical logs of activity, which would be overwhelming and hard to understand, a simple summary can highlight exactly what is relevant to people.

> ### FACEBOOK'S APPROACH
>
> Facebook has developed simple summary interfaces for privacy disclosures for years, including its "Why Am I Seeing This?[44] tools. The "Why am I seeing this post" and "Why am I seeing this ad" tools appear in-context, meaning that people can simply tap on posts and ads to get information about why they are appearing and take action to better personalize what they see.



2:04

Only you can see this

Why You're Seeing This Post

You're friends with **Eric Cheng**
Your friend since May 2008

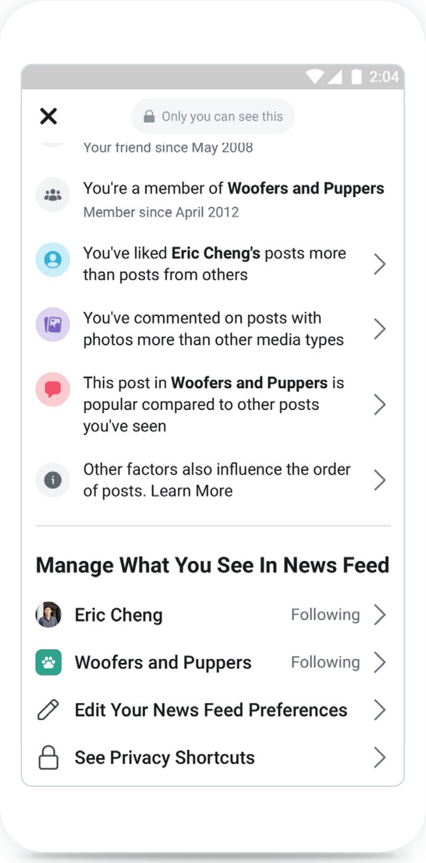
You're a member of **Woofers and Puppers**
Member since April 2012

You've liked **Eric Cheng's** posts more than posts from others

You've commented on posts with photos more than other media types

This post in **Woofers and Puppers** is popular compared to other posts you've seen

Other factors also influence the order of posts. Learn More



2:04

Only you can see this

Your friend since May 2008

You're a member of **Woofers and Puppers**
Member since April 2012

You've liked **Eric Cheng's** posts more than posts from others

You've commented on posts with photos more than other media types

This post in **Woofers and Puppers** is popular compared to other posts you've seen

Other factors also influence the order of posts. Learn More

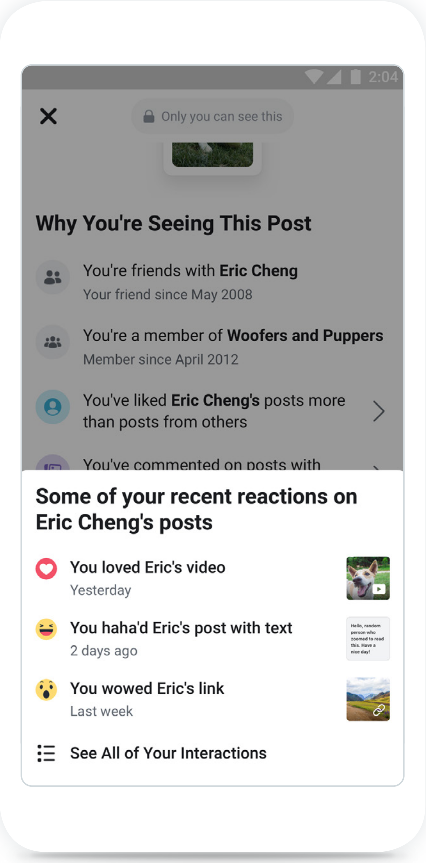
Manage What You See In News Feed

Eric Cheng — Following

Woofers and Puppers — Following

Edit Your News Feed Preferences

See Privacy Shortcuts



2:04

Only you can see this

Why You're Seeing This Post

You're friends with **Eric Cheng**
Your friend since May 2008

You're a member of **Woofers and Puppers**
Member since April 2012

You've liked **Eric Cheng's** posts more than posts from others

You've commented on posts with

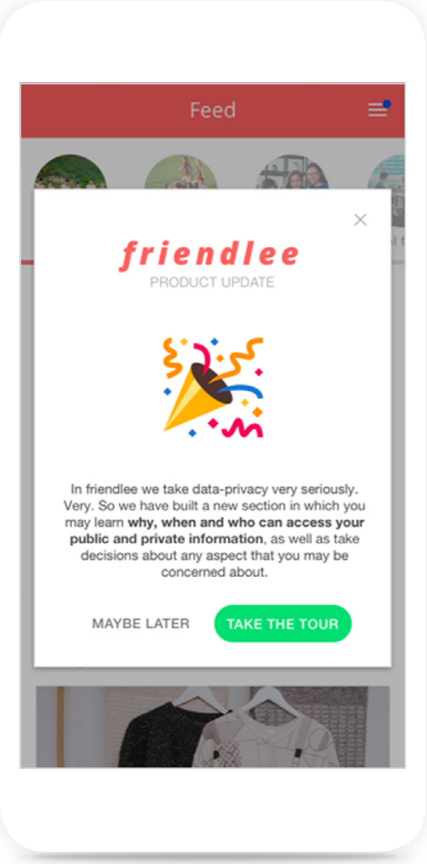
Some of your recent reactions on Eric Cheng's posts

You loved Eric's video
Yesterday

You haha'd Eric's post with text
2 days ago

You wowed Eric's link
Last week

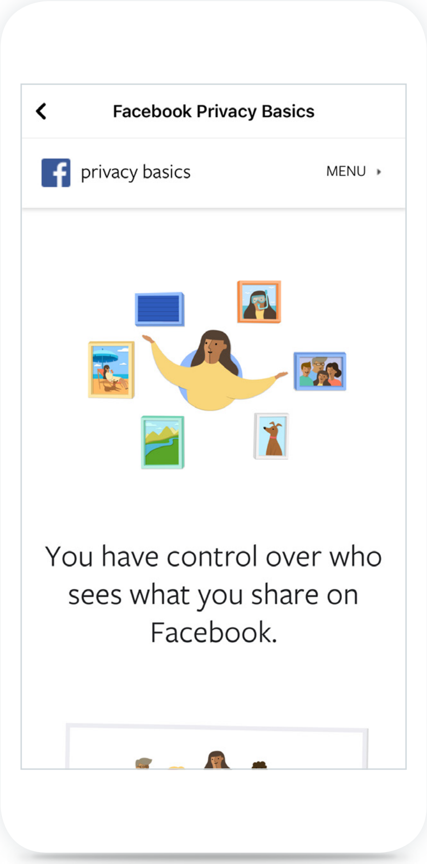
See All of Your Interactions



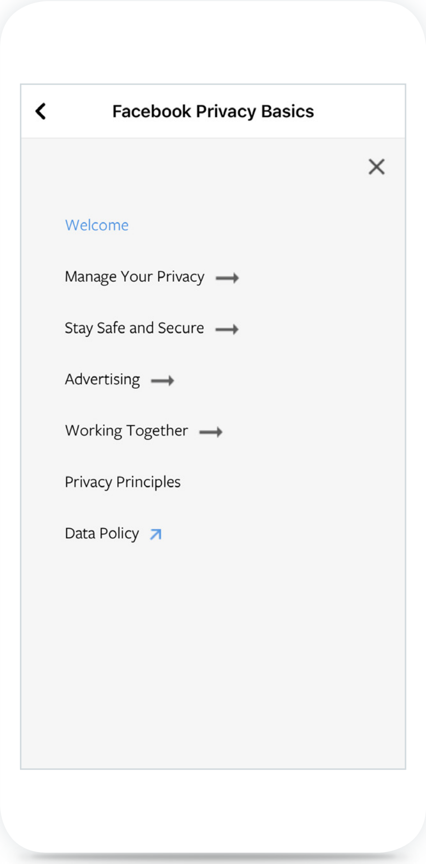
In friendlee we take data-privacy very seriously. Very. So we have built a new section in which you may learn **why, when and who can access your public and private information**, as well as take decisions about any aspect that you may be concerned about.

Progressive Disclosure

Progressive disclosure is the intentional sequencing of information and actions across several screens or interactions, rather than explaining everything during the onboarding process when people may be overwhelmed with the amount of reading they must do. The goal is to aid comprehension and decision-making. People see a high-level overview first, then continue moving through additional steps, learning as they go. Instead of communicating privacy policy changes as one-time upfront notices, people would be notified through in-app updates with clear designs and open language to help them understand the implications of permitting access to their data. People can 'take a tour' of new changes including what is being used and why, enabling more informed consent decisions.



You have control over who sees what you share on Facebook.



FACEBOOK'S APPROACH

Facebook has implemented progressive disclosures, including Privacy Basics,[45] which includes 32 interactive guides available in 44 languages. The guides use conversational language, illustrations of our privacy interfaces, and step-by-step walkthroughs to answer some of the most common questions we receive on privacy.

END NOTES

Communicating About Privacy: Towards People-Centered and Accountable Design

[1] Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 Stan. Tech. L. Rev. 74, 77 (2018), https://law.stanford.edu/wp-content/uploads/2018/03/Waldman_Final_031418.pdf.

[2] Alecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & Pol'y for Info. Soc'y 543, 563 (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

[3] Layered privacy policies, just-in-time notices, and in-context notifications can improve the usability of privacy notices for users. Layered privacy policies "constitute a set of complementary privacy notices that are tailored to the respective audience and the prevalent contexts in which they are presented. . . . For example, a full privacy policy can be complemented by short and condensed notices summarizing the key data practices." *See* Florian Schaub et al., *A Design Space for Effective Privacy Notices*, Proc. 11th Symp. Usable Security and Privacy 5 (2015) [hereinafter "*A Design Space*"], https://www.ftc.gov/system/files/documents/public_comments/2015/10/00038-97832.pdf. Just-in-time notices provide notice to users about specific data practices "at the point in time when it matters" to them, such as prior to sharing certain personal information. Fed. Trade Comm'n ("FTC"), Mobile Privacy Disclosures: Building Trust Through Transparency 15 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. Similar to just-in-time notices, in-context notifications may involve additional notices in contexts that are relevant to users, which "may be determined by a change in location, additional users included in or receiving the data, and other situational parameters." Schaub et al., *A Design Space*, *supra* at 7.

[4] *See, e.g.*, Personal Data Protection Commission Singapore, *Guide to Notification* (Sept. 26, 2019), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Notification-260919.pdf.

[5] *See, e.g.*, United Kingdom Information Commissioner's Office ("Information Commissioner's Office"), *Age-appropriate design: a code of practice for online services*, 39 (Jan. 22, 2020), https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-0-0.pdf. ("You should present . . . information in a way that is likely to appeal to the age of the child who is accessing your online service. This may include using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest children, rather than relying solely on written communications.").

[6] Lesley Fair, *Full Disclosure*, FTC Bus. Blog, (Sept. 23, 2014, 11:32 AM), www.ftc.gov/news-events/blogs/business-blog/2014/09/full-disclosure.

[7] Article 29 Data Protection Working Party, WP 260, *Guidelines on Transparency under Regulation 2016/679*, 17 (Apr. 11, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[8] *See generally* McDonald et al., *supra* note 2 at 549 (describing the "economics" of privacy policies).

[9] Organization for Economic Cooperation and Development ("OECD"), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Guidelines 12 & 13 (originally published 1980, updated 2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[10] *See* Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28 January 1981, as modernized in the 128th session of the Committee of Ministers (Elsinore, Denmark, 17–18 May 2018) ("Personal data undergoing processing shall be processed fairly and in a transparent manner."), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

END NOTES

11. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, art. 10–11.

12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119/1, art. 12 [hereinafter "GDPR"].

13. *See*, *e.g.*, Mike Hintze, In Defense of the Long Privacy Statement, 76 Md. L. Rev. 1044 (2017), https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3762&context=mlr.

14. *See* Waldman, *supra* note 1 at 94, n.103 (2018) (citing authorities requiring understandable notices).

15. *See* Cal. Bus. & Prof. Code § 22575(b)(1), (b)(3) (requiring privacy notice link to be posted clearly and conspicuously).

16. *See*, *e.g.*, Patrick Gage Kelley et al., *A 'Nutrition Label' for Privacy*, Symp. Usable Privacy and Security (2009), https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.

17. Florian Schaub et al., *Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making*. 14 IEEE Pervasive Computing 34 (2015), https://www.computer.org/csdl/magazine/pc/2015/01/mpc2015010034/13rRUwjXZPE.

18. GDPR, art. 13(2)(f) (requiring notification of the existence of automated decision-making and meaningful information about the logic involved); Id., art. 13(1)(f) (requiring notification of the fact that the controller intends to transfer personal data to a third country).

19. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, (2011), 140(4) Daedalus 32, 36 (adding "[t]hus the transparency paradox: transparency of textual meaning and transparency of practice conflict in all but rare instances. We seem unable to achieve one without giving up on the other, yet both are essential for notice-and-consent to work."), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567042.

20. *See* Article 29 Data Protection Working Party, WP 259, *Guidelines on Consent Under Regulation 2016/679*, 17 (Apr. 10, 2018), ("In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing."), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

21. *See* European Commission Press Corner, *Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions*, (Jan. 10, 2017) (observing that "[t]he so called 'cookie provision' [in Europe's ePrivacy Directive] … has resulted in an overload of consent requests for internet users"), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_16.

22. Schaub et al., *A Design Space*, *supra* note 3 at 9 ("Presentation and layout are important aspects in the design of visual notices, including colors, fonts, and white space, all of which can impact users' attention and comprehension of the notice.").

23. *See* Waldman, *supra* note 1 at 113.

24. For example, the statutory text of the California Consumer Privacy Act requires certain companies to post a "Do Not Sell My Personal Information" button on their websites. Cal. S. B. 1121 (2017-2018) §8(a) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121; Cal. Civ. Code §1798.135(a) (effective Jan. 1, 2020).

25. *See*, *e.g.*, GDPR art. 12 (empowering the European Commission to "adopt delegated acts . . . for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons."); APEC Privacy Framework §II(21-23) (2015) ("To provide notice on small screens, personal information controllers may want to consider the value of standard notices, icons, or other measures."), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015); Text of Modified Regulations [Clean Version] § 999.306(f), Cal. Dep't Justice (Jan. 2020) (mandating a specific design for an opt-out button), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

26. *See*, *e.g.*, Rishab Bailey et al., *Disclosures in privacy policies: Does 'notice and consent' work?*, Nat'l Inst. Pub. Fin. and Pol'y 8 (Dec. 2018), https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf. ("The peculiarities of the Indian context throw up new challenges of diversity in language, literacy, modes of Internet access and other variations among the over 494 million Internet users in India. All of these factors will have to play a role in determining the appropriate design of disclosures and consent frameworks for Indian users.").

27. OECD, *Recommendation of the Council on Artificial Intelligence* (May 21, 2019) [hereinafter "OECD Recommendation"], §1.3, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. In addition to the OECD Recommendation, there are an increasing number of legislative proposals and guidance documents that aim to promote transparent and explainable algorithmic decision making. Information Commissioner's Office, *Draft Guidance on Explaining Decisions Made by AI* (Jan. 24, 2020), https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-and-the-turing-consultation-on-explaining-ai-decisions-guidance/; Algorithmic Accountability Act of 2019 (S. 1108 116th Cong. (2019); H.R. 2231, 116th Cong. (2019)); European Union European Commission, *Ethics Guidelines for Trustworthy AI* (April 8, 2019), https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai; Innovation, Science and Economic Development Canada, *Proposals to Modernize the Personal Information Protection and Electronic Documents Act ("PIPEDA")* (May 21,2019) (proposing to revise PIPEDA to requiring informing individuals about the factors involved in automated decision-making), https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

END NOTES

[28] Leilani H. Gilpin, et al., *Explaining Explanations: An Overview of Interpretability of Machine Learning*, Computer Sci. and Artificial Intelligence Lab. M.I.T. 1 (Feb. 3, 2019) ("In order for humans to trust black-box methods, we need *explainability*—models that are able to summarize the reasons for neural network behavior, gain the trust of users, or produce insights about the causes of their decisions."), https://arxiv.org/pdf/1806.00069.pdf.

[29] It should be noted that some argue that because there is a limit to the detail with which advanced technologies can be effectively explained, other methods of accountability should be explored. *See, e.g.*, Mike Ananny & Kate Crawford, *Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, New Media & Soc'y 12 (2016), http://mike.ananny.org/papers/anannyCrawford_seeingWithoutKnowing_2016.pdf.

[30] The Alan Turing Institute and United Kingdom Information Commissioner's Office ("Information Commissioner's Office"), *Explaining decisions made with AI*, 20 (May 20, 2020), https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf.

[31] Virtual reality has been defined as a fully immersive software-generated artificial digital environment. and augmented reality has been defined as an environment in which digitally-created content is overlayed on a person's real-world environments, viewed through a device (such as a smartphone) that incorporates real-time inputs to create an enhanced version of reality. Kavya Pearlman et al., XR-001, *The XRSI Definition of Extended Reality*, XR Data Classification Framework P Working Group (Oct. 2019), https://www.xrsi.org/wp-content/uploads/2019/10/RFC-XR-DCF-Special-Publication-0001.pdf.

[32] Mark Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. of Pa.. L. Rev. 1051, 1125 (2018), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9622&context=penn_law_review.

[33] The OECD recently published a policy paper exploring the role of sandboxes in promoting flexibility and innovation in the digital age broadly speaking. OECD, *Chapter 4. Unleashing Innovation*, Going Digital: Shaping Policies, Improving Lives, https:/www.oecd-ilibrary.org/sites/c285121d-en/index.html?itemId=/content/component/c285121d-en; Centre for Information Policy Leadership: Hunton Andrews Kurth, *Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice* (Mar. 8, 2019), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

[34] For example, the UK Information Commissioner's Office has set up a sandbox to "help companies and public bodies deliver new products and services of real benefit to the public, with assurance that they have tackled built-in data protection at the outset." Information Commissioner's Office, *The Guide to the Sandbox (Beta Phase)* (2019), https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/. In addition, the Singapore Personal Data Protection Commission has announced it is "prepared to work with organisations to create regulatory sandboxes that will allow them to move faster, and at the same time, allow [the PDPC] to understand how our proposed changes to the PDPA might work in practice . . . ." Personal Data Protection Commission Singapore, *Data Sharing Arrangements* (Feb. 8, 2018), https://www.pdpc.gov.sg/Legislation-and-Guidelines/Exemption-Requests/Data-Sharing-Arrangements.

[35] "Design Jams" are interactive one-day workshops on issues of trust, transparency and control in the digital space. They bring together diverse stakeholders with different viewpoints. These stakeholders share ideas, develop new perspectives and create digital prototypes that bring their ideas to life.

[36] For more information about TTC Labs and Design Jams, *see infra*, *App'x B*.

[37] *See* toolkit.ttclabs.net/research/people-centric-approaches-to-notice-consent-and-disclosure.

[38] *See supra* notes 4-7, above.

[39] Dark Patterns are "interface designs that try to guide people into desired behaviour through malicious interaction flows" and can be abused by bad actors seeking to profit from the imbalance of information about where and when data is being collected. *See* Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, Chi Conference on Human Factors in Computing Sys. 3 (Apr. 2020), https://arxiv.org/pdf/2001.02479.pdf.

[40] *See* Centre for Information Policy Leadership: Huntons Andrews Kurth, *Organisational Accountability - Past, Present, and Future*, 2, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organisational_accountability_%E2%80%93_past_present_and_future.pdf.

[41] *Id.*, at 3-4.

[42] *See* Facebook Newsroom, *Privacy Checkup Is Now Rolling Out* (Sept. 4, 2014), https://about.fb.com/news/2014/09/privacy-checkup-is-now-rolling-out/.

[43] *See* Facebook Newsroom, *Guiding You Through Your Privacy Choices* (Jan. 6, 2020), https://about.fb.com/news/2020/01/privacy-checkup/.

[44] *See* Facebook Newsroom, *Why Am I Seeing This? We Have an Answer for You* (Mar. 31, 2019), https://about.fb.com/news/2019/03/why-am-i-seeing-this/.

[45] *See* Facebook Newsroom, *Introducing the New Privacy Basics* (Jan. 26, 2017), https://about.fb.com/news/2017/01/introducing-the-new-privacy-basics/.