PRIVACY & SECURITY BY DESIGN

Best Practices for Collecting and Protecting User Data

Reese Legal Team | 2018

UNC SCHOOL OF LAW

PRIVACY & SECURITY BY DESIGN

Best Practices for Collecting and Protecting User Data

No matter what your product is, whether it be an app to inform users on local elections, or a payment service for 20-something drinkers trying to avoid long lines at the bar, you will likely be collecting information from your users. Collecting information about your users allows you to better personalize services and marketing, and sharing the information in an appropriate way could potentially be a revenue stream for your company. Almost all websites—including the Federal Trade Commission's, the federal agency that polices private companies' cybersecurity—collect some information on its visitors. But startups should tread carefully. Successful tech companies ranging from Uber to Google to Facebook have gotten into trouble with the FTC and have lost public trust for mishandling user data. **It is important to think about users' privacy throughout your product design and development process.**

So exactly how much information should you collect, what can you do with that information, and how do you protect that information? These FAQs on **collecting, protecting** and **sharing** user information will help you create privacy by design in your product, and to assure that your users understand what you are doing with their information.

COLLECTING INFORMATION

1. I want to collect personally identifiable information, like a user's name, birth date, and address. Is this OK?

Federal regulators, like the FTC, expect mobile app developers to **adopt and maintain reasonable data security measures if the app will collect any personally identifiable information about its users**; however, there is no one-size-fits-all approach to what information is appropriate to collect and what information is not.

In determining what information to collect from your users, **the rule of thumb is to not collect or store data that you do not need for your app to be successful**. Remember, if you do not collect the information at all, you don't have to take the effort to secure it. However, if certain personally identifiable information is required or is integral to the business model for your product or service, collecting this information is fine, so long as you take reasonable steps to secure the data and delete the data once you no longer have a legitimate business need to retain it.

For more information, check out these FTC Best Practices, which are written for mobile health app developers, but applicable to any mobile app.

2. I plan to require users to create usernames and passwords to use certain functions of the app. Are there any privacy issues to consider?

If you plan to create user credentials, like usernames and passwords, create them securely based on the type of app you intend to create. For example, the method for authenticating a user on a game app may not be secure enough for authenticating a user on a social media website.

Also, it is best not to store passwords or other collected user data in plaintext on your company's servers because, in the event of a data breach, intruders have unrestricted access to all unencrypted data. Uber recently came under FTC fire after intruders hacked into Uber's cloud storage and downloaded files containing millions of users' names, passwords, email addresses, mobile phone numbers, and the driver's license numbers of 600,000 U.S. Uber drivers that were stored in plaintext. Uber had to renegotiate its settlement with the FTC and subject itself to additional civil penalties and stricter privacy requirements as a result of this data breach.

To avoid this same fate, consider encrypting user passwords and other collected user data on your servers. Then, if your server suffers a data breach, passwords and other sensitive data are not left completely exposed.

3. I plan to access other functions of a mobile device, like the user's contacts, camera, or maps. Can I do this?

Some app designs require access to other functions of a mobile device, like the camera or maps, to fulfill the purpose of the app. However, make sure your app doesn't access more functions of the mobile device than needed for the app to work. For example, if you're developing a fitness app, consider whether the app really needs access to other functions, like the camera or the user's contacts. If not, your app should not access that information.

If your app does require use of other functions, make sure this is clearly disclosed in the privacy policy or terms of use. Mobile advertising company InMobi had to pay the FTC $950,000 in civil penalties after the agency discovered the company tracked consumers' location information without users' consent. The FTC alleged InMobi misrepresented that it only tracked consumers' location when a user opted in through one of their mobile apps; however, according to the FTC, the company tracked consumer locations through use of the mobile map functions, whether or not the apps using InMobi software asked for permission to do so, and even when consumers denied permission.

Consider providing users a way to affirmatively consent to allowing your app to access additional apps or functions of their mobile device. Additionally, if a user opts to deny permissions, honor that denial and do not continue to access other aspects of the mobile device.

4. I plan to use in-app purchases. Are there any privacy or data security issues to consider?

Collecting user payment information can be complicated. To accept payment through your mobile app, you must secure your user's financial data in a way that adheres to the PCI compliance standards. The PCI standards are a set of security standards designed by various credit card companies to widely incorporate payment card industry standards to ensure the safety of cardholder data. If you are a merchant accepting credit cards, you must be in compliance with the compliance standards.

The PCI standards require merchants to encrypt transmission of cardholder data across open, public networks; restrict access to cardholder data to only essential personnel; and track and monitor all access to network resources and cardholder data. The PCI standards also recommend only storing payment information or cardholder data when there is a necessary business reason to do so. Mobile apps that do not automatically store cardholder data decrease their risk of a possible data security breach.

You can also outsource all payment processing by using a mobile payment widget, offered by companies such as PayPal or Stripe. This requires less work on your part to be PCI compliant, although you will still have to validate your compliance with PCI annually.

In addition, the FTC encourages apps offering mobile payment services to disclose their users' rights and liability limits for unauthorized, fraudulent, or erroneous transactions in the app's terms of use. For more information, visit the PCI website and FTC guidance concerning mobile payment services.

5. How should I inform users about the data the app plans to collect, how it will be used, and how it will be secured?

The best place to inform users about the data your app collects, how it will be used, and how it will be secured, is in your app's privacy policy or terms of use. The privacy policy should tell users about any sensitive or unexpected data that will be collected both when the app is installed and as the app is used. In disclosing what data is collected, it is important to be as clear and direct as possible. Don't complicate the privacy policy with legal jargon or hidden hyperlinks with essential information.

It also may be wise to get a user's express permission or consent before collecting the sensitive user data. For example, one way of obtaining consent is having the users indicate "yes" or "I agree" to your privacy policy before collecting the users' information. Federal regulators also advise making the privacy policy or privacy disclosures available both before the user installs the app and again when the app begins to collect the data to provide what is called "just in time" notice.

Also, industry best practices suggest explaining why you are collecting the user's data in your privacy policy. Users may be less suspicious of your data collection practices if they understand the purpose behind it.

Whenever and however you choose to inform you users of your data collection practices, make sure your disclosures are truthful about the information your app collects. Regulating agencies and private individuals have sued companies over false or deceptive data collection policies. Recently, Snapchat settled charges with the FTC after the agency alleged that the app collected information from users' contacts and address books without notice or consent.

SHARING INFORMATION

1. I want to work with a third party to manage and analyze users' data. What should I be looking for in a third-party storage company?

It is relatively common practice for apps to use third-party companies to store and analyze user information. **Before giving your users' information to a different company, research the company and its privacy policy to make sure it is not mishandling data, and that the company**

does not use the information in an inappropriate way. Some third-party companies sell the information for targeted ad services, so make sure that the company either does not resell the data or provides an opt-out option. Also, be sure to check in periodically to make sure that the company abides by the agreement and is not misusing the data—think Facebook and its Cambridge Analytica debacle, in which Facebook did not realize Cambridge was collecting and using information far beyond the scope of the agreement because Facebook did not regularly check to make sure apps complied with its rules. Of course, be sure to tell users in the terms of use that their information is shared with the third party, and link to the company's privacy policy in your terms of use. For more information, check out these guidelines on Best Practices for Mobile App Developers.

2. What if I want to sell my users' information as a way to make money?

The more you allow outsiders to access your users' data, the more you will be exposing your company to legal risks. You could be liable if the third party uses the data illegally or does not properly secure the information. For example, in 2012 the FTC brought an action against Spokeo for "compiling and selling people's personal information for use by potential employers in screening job applicants" in violation of the Fair Credit Reporting Act. Within the list of grievances, the FTC charged Spokeo for failing to make sure that subscribers were using the information legally, and it failed to tell the subscribers what their legal obligations were. As with third-party storage companies, make sure both you and your consumers know what the buyer is doing with the data, and check in periodically to make sure the buyer is not changing its practices.

It is less risky to sell user data in an aggregated and de-identified format. You can see in this compilation of popular apps' privacy policies that Spotify, Tinder, and Lyft reserve the right to sell non-personal, anonymized user data to third parties in their terms of use. The FTC says that information is considered de-identified if "a company takes reasonable measures to de-identify the data, commits not to re-identify it, and prohibits downstream recipients from re-identifying it." However, it is still important to make sure that you provide notice and get users' informed consent beforehand. Unroll.me, a service that users could download to unsubscribe to email lists, collected information on users' email receipts, then sold the information to third parties. Even though the information was anonymized and the Unroll.me's privacy policy stated "we may collect, use, transfer, sell, and disclose non-personal information for any purpose," people were upset when it was revealed in April 2017 that it would scour people's emails for Lyft receipts and sell the info to Uber. Unroll.me apologized for not being "explicit enough," and the company was sued for not adequately informing users about this business practice.

Be as transparent and explicit as possible with your users to make sure they understand who is buying the information and for what purposes. This Forbes op-ed provides other important business considerations for selling user data, such as how much money you can make and how it might affect consumers' trust.

3. How careful do I need to be with contractors and employees accessing user data?

In North Carolina, the authorized access of personal information by an employee or agent is not considered a security breach so long as the information is used for a lawful purpose. It is important to disclose in your company's privacy policy that the information will be accessible to contractors and employees. When your company grows up, it would also be smart to include language in contractor agreements that requires the contractor to uphold standard and reasonable cybersecurity practices and have data breach insurance. This language can place the risk of a breach that occurs from third-party access on the contractor and could be very helpful if a breach occurred.

4. My app is already up and running, and I have a great idea for a new product using data I've already collected. Can I do this?

Before doing anything new with previously collected user information, **review your terms of use and consider if the new use is in conformity with your data policies.** If it is not, get affirmative, opt-in consent from your users before moving forward with your new idea. Also, be sure that users who opt out are left out of the new data changes. Google got in trouble with the FTC for asking Gmail users if they wanted to participate in a new chat feature called Buzz, and those who opted out still were enrolled in some of the Buzz features. The FTC's action against Google also charged the company failed to let users know that their most frequent email contacts would be public by default, which for some people included "ex-spouses, patients, students, employers, or competitors." So before making changes, think about whether (1) you are getting full, informed consent to move forward, (2) you are allowing users to opt-out, and (3) you could be inadvertently revealing new personal information about your users that might upset them.

5. I've seen some really cool patterns in user activities, and I want to write a blog post about it. Any legal concerns?

Start with your terms of use and make sure that you have already told users that you might share their information. If you have not done so already, make sure to get consent from the users beforehand. Assuming that this information will be anonymized, consider if a determined reader might be able to re-identify the user's data based on what you are presenting to them. In 2006 AOL published anonymized search histories for more than 650,000 users over a three-month period of time, and the *New York Times* was able to identify one elderly woman from Lilburn, Georgia based on her searches. Users sued in a class action lawsuit, claiming that people's identities could be discerned by the released information and this violated privacy and consumer protection laws. AOL ended up settling for $5 million. Netflix also published roughly 500,000 customers' movie rental histories with random numbers associated with each customer, and it also settled a privacy lawsuit after researchers were able to re-identify some of the user data.

The more data points you provide, the more likely it is that the information may be re-identified. Researchers in one study found that 63% of people could be reidentified based on just their date of birth, gender and zip code. Also, keep in mind that a smaller pool of people would be more easily re-identified than a larger pool, so effective anonymization of user data for Uber might not work for a smaller company. Going to the general theme of privacy and security by design, to reduce the risk that personal information may be re-identified, do not release more information than necessary to make your point, and make sure that you have obtained consent to release this information.

PROTECTING DATA

1. What should I do for my application's cybersecurity?

The appropriate level of cybersecurity efforts for any given company largely depends on the type of information being collected, the standards in the company's industry, and the generally reasonable options to improve the security messages readily. **A company should try to keep their cybersecurity practices up to par with other similarly structured businesses, given the resource constraints of the company.** Unfortunately, in the beginning, many startups take shortcuts and huge risks until they have the resources to figure it out. A company must implement reasonable cybersecurity measures that match its privacy policies and terms of use to avoid liability. Companies and agencies often reference the NIST Cybersecurity Framework, which provides general guidance for all companies. Protection by design can become a corporation's best friend to ensure cybersecurity measures are in place early on to avoid negligence-based liability for a breach.

There are two main ways to shield your computer systems and apps from cyber-attacks: (1) protect the internal server's integrity or (2) protect communications over the internet with end-to-end or Point to Point ("P2P") encryption **Protection by design can be implemented through features like**: multi-factor authentication; end-to-end encryption; at rest encryption; breach alerting; activity monitoring; and malware software can all protect the system from breach. For more information, read up on these methods and more here.

2. This is overwhelming. Can I get professional help to make my service secure?

The best way to get professional help is to hire someone from with experience in the field to work with your application development and operations teams. Sometimes startups attempt to start an application with an outsourced development team and then to save money bringing maintenance and cybersecurity in house. **However, privacy and security are best created and implemented internally rather from the beginning than outsourced**. One 2013 study found that 63% of breaches were linked to outsourced IT security. As this article asserts, outsourcing cybersecurity decisions leads to data breaches because giving another party access to your users' data creates another vulnerable point for cyber-attacks. The best way to protect data is by bringing these choices in-house and limiting access to sensitive information to as few parties as possible. Ritwik Pavan, UNC alum and Founder of Linker Logic Technologies, says the company's own application backend or database developer should be the person responsible for the database's security and design, and a quality assurance tester should test the system's integrity. The quality assurance testing is generally done in-house but may also be done through a third-party vendor. Generally, the more security design and programming is done in-house from the beginning, the more effective the security. Ironically, companies often increase risk exposure by outsourcing quality assurance and routine risk analysis. In summary, outsourcing the responsibility of data security for an application is probably not the best solution and increases unnecessary vulnerabilities.

Implementing these security measures at the early stages of app development and in-house is much more effective and cost-efficient way to achieve effective cybersecurity practices.

3. What do I do if I have a breach?

Forty-eight states have passed different data breach notification laws, so a company's response should vary depending on the states customers are located. However, the general consensus is that after a data breach, a company should notify the exposed customers reasonably soon after the breach is discovered. This condition is only triggered in North Carolina if the exposed information is personal information that is not encrypted or redacted. Personal information includes an individual's driver's license number, credit/debit card number, or any number that can be used to access an individual's financial resources. However, if you only collect publicly available information, or information that is not personally identifiable, you are outside the purview of most states' data breach laws, including North Carolina's law.

In North Carolina the notice to exposed customers must include: (1) general description of the security breach incident; (2) type of personal information breached; (3) general description of your efforts to avoid further unauthorized access to personal information; (4) telephone number where people can call for more information and assistance, if one exists; and (5) advice for people who are affected. Other states have similar requirements that are constantly evolving, so if you get a national consumer base and are collecting sensitive information, it would be best to talk to an attorney.

SO, WHAT'S THE TAKEAWAY?

To sum it all up, do not collect more information than you need to run your app, and provide notice and obtain consent for all uses of your users' data. The most crucial step in assuring you are implementing privacy and security by design is through well-drafted privacy policy terms explaining what data you collect, how you use it, and with whom you share it. Below are more resources to guide you as you navigating collecting and protecting user data in a legal and ethical way. If you come across a tough question, ask people with more experience in the industry, and run it by a lawyer.

For more information:

- Entrepreneur, 10 Questions to Ask When Collecting Customer Data
- Future of Privacy Forum and Center for Democracy & Technology, Best Practices for Application Developers
- ABA, Hey, that's personal! When companies sell customer information gathered through the Internet
- FTC, App Developers: Start with Security
- NCDOJ, North Carolina's Security Breach Information
- Computer Weekly, Bad Outsourcing Decisions Cause 63% of Data breaches

Note: The contents of this document are intended to convey general information only and not to provide legal advice. Please consult an attorney for specific legal questions.