

How To Avoid Becoming The Next Facebook Privacy Problem

Six Critical components of a company privacy policy

Facebook recently divulged that the personal data of up to 87 million users may have been improperly shared with a third party.

The scandal publicized Facebook's collection of very personal user data. Users around the world were shocked by the revelation and have rallied against the company and its executives. Recently, Facebook CEO Mark Zuckerberg was questioned and criticized in a congressional hearing about the company's policies regarding user data. This recent attention to Facebook's policies has consumers asking how companies use their data. It may also leave companies wondering whether to review and revise internal policies regarding customer data.

Although few companies collect the breadth of personal data held by Facebook, almost every company collects some personal data from customers.

As companies increasingly (and sometimes exclusively) conduct business over the internet, it is critical that a company maintain a comprehensive privacy policy. A privacy policy, sometimes referred to as a privacy notice, is an external-facing policy, often posted to a company's website, that discloses to customers the ways in which data are gathered, obtains consent when appropriate, and permits an individual to manage or delete information once it has been collected.

Why you need a privacy policy

Most states, including Wisconsin, do not require companies to have privacy policies. However, some states, including California, require that companies doing business in that state adopt a privacy policy.

Therefore, if a Wisconsin company's website can be accessed by users or customers in a state which requires a privacy policy, that company must adopt a privacy policy. Also, some federal laws, including the Health Insurance Portability and Accountability Act, require that a company adopt a privacy policy. If a

POSTED:

May 2, 2018

RELATED PRACTICES:

[Corporate Law](#)

<https://www.reinhartlaw.com/practices/corporate-law>

RELATED SERVICES:

[Data Privacy and Cybersecurity](#)

<https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity>

RELATED PEOPLE:

[Melissa A. Zabkowicz](#)

<https://www.reinhartlaw.com/people/melissa-zabkowicz>

company engages in an industry regulated by federal law – healthcare, for instance – that company is required to adopt a privacy policy. Various international laws, like the EU’s General Data Protection Regulation, also require the use of privacy policies.

Because these laws are so pervasive, it’s likely that some aspect of a company’s business will require the company to adopt a privacy policy.

The six components of a privacy policy

In light of the recent privacy scandal at Facebook, consumers have become increasingly aware of the scope of companies’ collection and use of their personal data. Most users know that some of their data will be collected—so transparency and honesty are critical.

Companies should consider doing these six things with their privacy policies:

1. **Provide notice:**

A privacy policy should inform customers of the types of personal data that are being collected. For example, if a company is collecting its customers’ names, addresses, e-mail addresses, phone numbers, login information and payment-card information, customers should be notified. As discussed below, a good privacy policy should also state that if customers access the company’s “pages” on social media sites like Facebook, Twitter and Instagram, that social media site’s policy, and not the company’s policy, governs the collection of the personal data.

2. **Explain how data will be used:**

Policies should explain to customers how their data will be used by the company. For example, companies should inform customers if they are using data for processing payment transactions, sending marketing communications, or personalizing customers’ experience. Policies should also state whether customers’ data are being provided to third parties.

3. **Make data accessible**

Third, policies should allow customers to access and review data that are being collected. For example, a privacy policy might provide customers with a link and step-by-step instructions to a specific website where a customer’s data can be accessed. Alternatively, companies can direct customers who want more information to send an e-mail or submit an

online form.

4. **Allow choices regarding data collection and use**

A policy should provide customers options concerning how data are collected and used. For example, companies should give customers an avenue with which to delete or modify any personal data from their systems. Companies may also inform customers when they will respond to a delete or edit request. If they are unable to respond within the stated time, they should provide customers with an explanation. Many companies also remind customers that they may un-enroll from receiving e-mail advertisements by following a link at the bottom of those same e-mails.

5. **Communicate security standards**

Companies may use a privacy policy to explain to customers whatever steps are being taken to protect personal information and ensure it will not fall into the wrong hands. Any statements on security measures should remain broad rather than specific and technical. But a company may want to inform customers that it uses physical, technical, and administrative protections to secure data.

6. **Offer a means of redress**

Lastly, companies should provide customers with the contact information of a company representative who can help with any inquiries they might have, as well as concerns that privacy policies are not sufficient or are not being followed. This is a big step in gaining customers' trust.

Why your privacy policy should include social media interactions

Most companies have social media pages, and use those pages as a way to interact with customers. In fact, companies might get more traffic through social media than their own websites. Accordingly, it is imperative that companies' privacy policies include a statement regarding social media privacy.

The statement should make it clear that the privacy policy does not govern any of the company's pages on social media sites. For customers who want more information on those sites' policies, it's often best to refer them to the social media companies themselves.

Pitfalls of misleading privacy policies

If a company institutes a privacy policy, but fails to comply with that policy, it risks



violating Section 5 of the Federal Trade Commission Act, which prohibits unfair methods of competition and deceptive practices. Therefore, it is vital that a company's privacy policy be accurate in all respects. To ensure continued compliance, an individual at the company should be responsible for reviewing and revising the policy at least annually.

This [article](#) was originally published in the [Wisconsin Law Journal](#) April, 2018 edition.

These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.