

million are willingly sharing information that could be used against them in some way. That includes plans to travel on a particular day, which burglars could use to time robberies, or Liking a page about a particular health condition or treatment, which insurers could use to deny coverage. 13 million users have never adjusted Facebook's privacy controls, which allow friends using Facebook applications to unwittingly transfer your data to a third party without your knowledge. Credit card companies and other similar organizations have begun engaging in "weblining", taken from the phrase redlining, by altering their treatment of you based on the actions of other people with profiles similar to yours.

Ninety-three percent of people polled believe that Internet companies should be forced to ask for permission before using your personal information, and 72 percent want the ability to opt out of online tracking. Why, then, do so many people share sensitive details of their life on Facebook? Often it's because users do not realize that their data are being collected and transmitted in this way. A Facebook user's friends are not notified if information about them is collected by that user's applications. Many of Facebook's features and services are enabled by default when they are launched without notifying users. And a study by Siegel + Gale found that Facebook's privacy policy is more difficult to comprehend than government notices or typical bank credit card agreements, which are notoriously dense. Next time you visit Facebook, click on Privacy Settings, and see if you can understand your options.

Facebook's value and growth potential is determined by how effectively it can leverage the personal data is aggregated about its users to attract advertisers. Facebook also stands to gain from managing and avoiding the privacy concerns raised by its users and government regulators. For Facebook users that value the privacy of their personal data, this situation appears grim. But there are some signs that Facebook might become more responsible with its data collection processes, whether by its own volition or because it is forced to do so. As a publicly traded company, Facebook now invites more scrutiny from investors and regulators because, unlike in the past, their balance sheets, assets, and financial reporting documents are readily available.

In August 2012, Facebook settled a lawsuit with the FTC in which they were barred from misrepresenting the privacy or security of users' personal information. Facebook was charged with deceiving its users by telling them they could keep their information on Facebook private, but then repeatedly

allowing it to be shared and made public. Facebook agreed to obtain user consent before making any change to that user's privacy preferences, and to submit to bi-annual privacy audits by an independent firm for the next 20 years. Privacy advocate groups like the Electronic Privacy Information Center (EPIC) want Facebook to restore its more robust privacy settings from 2009, as well as to offer complete access to all data it keeps about its users. Facebook has also come under fire from EPIC for collecting information about users who are not even logged into Facebook or may not even have accounts on Facebook. Facebook keeps track of activity on other sites that have Like buttons or "recommendations" widgets, and records the time of your visit and your IP address when you visit a site with those features, regardless of whether or not you click on them.

While U.S. Facebook users have little recourse to access data that Facebook has collected on them, users from other countries have made inroads in this regard. An Austrian law student was able to get a full copy of his personal information from Facebook's Dublin office, due to the more stringent consumer privacy protections in Ireland. The full document was 1,222 pages long and covered three years of activity on the site, including deleted Wall posts and messages with sensitive personal information and deleted e-mail addresses.

It isn't just text-based data that Facebook is stockpiling, either. Facebook is also compiling a biometric database of unprecedented size. The company stores more than 60 billion photos on its servers and that number grows by 250 million each day. A recent feature launched by Facebook called Tag Suggest scans photographs using facial recognition technology. When Tag Suggest was launched, it was enabled for many users without opting in. This database has value to law enforcement and other organizations looking to compile profiles of users for use in advertising. EPIC also has demanded that Facebook stop creating facial recognition profiles without user consent.

In 2012, as part of the settlement of another class-action lawsuit, Facebook agreed to allow users to opt in to its Sponsored Stories service, which serves advertisements that highlight products and businesses that your Facebook friends are using. Now, users can control and see which of their actions on Facebook generate advertisements that their friends will see. Sponsored Stories are one of the most effective forms of advertising on Facebook because they don't seem like advertisements at all to most users. Facebook had previously argued that