Issued 5/24/10

Why You're Getting so Many Emails about Privacy Policies

Notice all those notifications you're suddenly getting about privacy policy updates from Facebook, Google, and multiple other companies? You can thank Europe for that. On May 25, the European Union is enacting the General Data Protection Regulation or GDPR, a new privacy law designed to make sure users companies to be transparent with what information they're gathering and why. Individuals get the right to access all their personal data, control access and use of it, and even have it deleted. The law will put data privacy and protection at the center of technology design — it can no longer be an afterthought. The law protects the citizens of the European Union's 28 member countries, regardless of where the data is processed or where the company collecting it is headquartered. In other words, any company or entity in the world — including banks, universities, social networks, tech platforms, and publishers — dealing with European citizens' data will need to comply. Designed to replace the European Union's previous governance dating back to 1995, the GDPR is the most sweeping overhaul of online primacy in more than two decades. It was approved by the EU Parliament in April 2016 and will go into effect on May 25, 2018. What the law does, essentially, is unify rules for how companies handle European citizens' data, expand the scope of what personal data is, strengthen transparency and consent conditions, and set specific penalties for enforcement. Among its requirements:

• Firms must notify users of a data breach within 72 hours of discovering it.
• They must request user consent in a clear, accessible way.
• They must allow data portability, meaning users can ask for a copy of their information and ship it off to others.

• The law also includes the “right to be forgotten” — meaning people can ask platforms to stop disseminating, halt third-party access to, or delete their data. Outlined in Article 17 of the law as the “right to erasure,” it allows people to request that an entity with their personal data delete it and not disseminate it further, so they can essentially take back their consent. The company in theory has to comply unless there is some public interest in the data (say, it’s a public figure, of historical use, etc.), but there is some debate about how it will be enforced. For example, if a public figure wants to have something from her past deleted, it’s not entirely clear whether she’ll be able to do that.

Companies that don’t comply or break the rules can face a steep fine of up to 4 percent of annual global revenue. For Facebook, that’s about $1.6 billion.