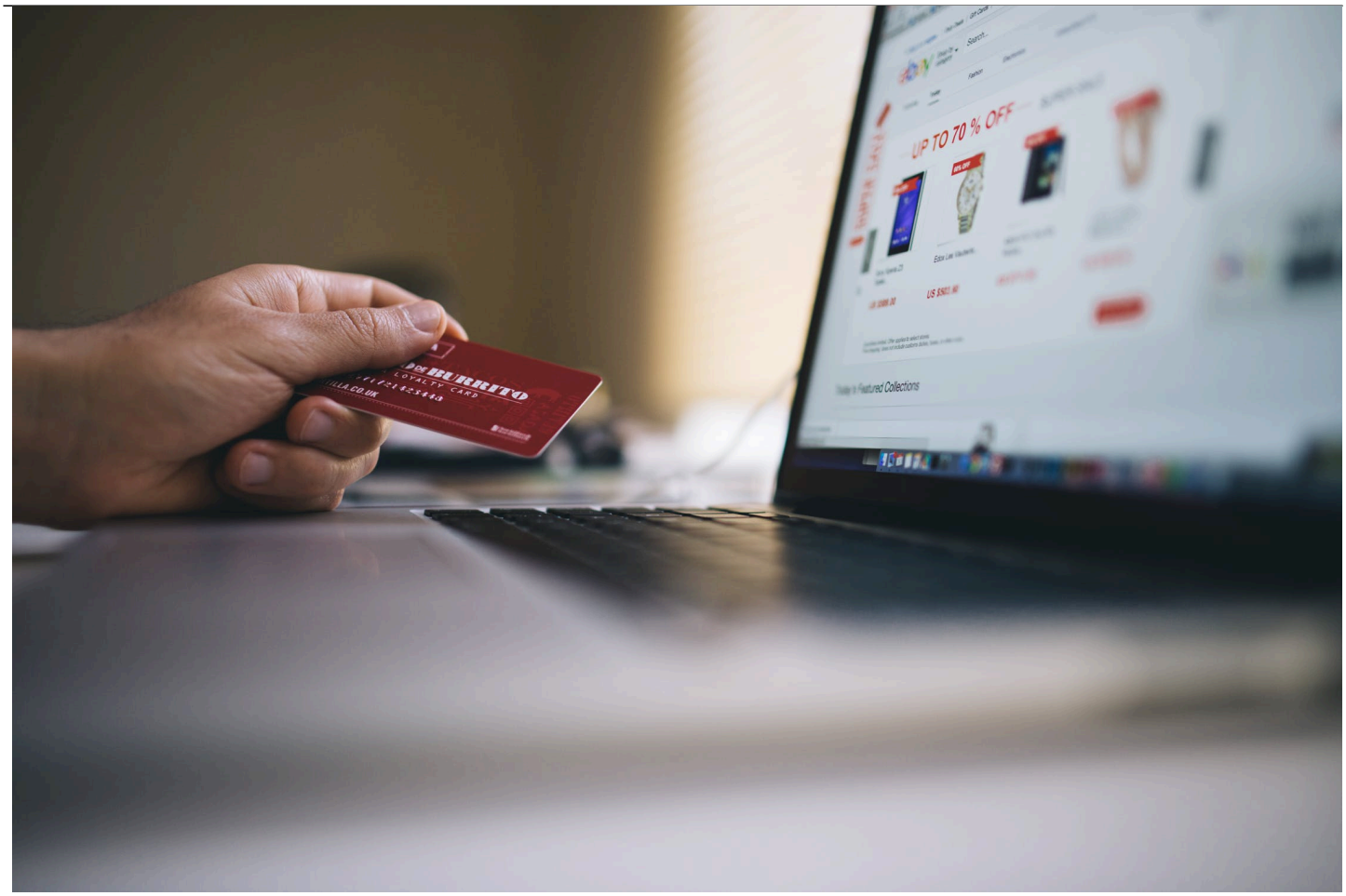
???????? 2019 ?????

???????? 2019 ?????

???Brian Byer



2018 was a year marked by privacy scandals in the tech sector. These scandals, which were the focus of much media attention and government scrutiny, have helped to make issues of online privacy and data security a point of greater concern for average consumers.

By now the general public has come to expect that data breaches can and will happen, and that hacking attempts by bad actors may sometimes leave their personal data exposed. The expectation, though, has previously been that such breaches were the result of accidental oversight or in some cases negligence, but that user data was not

exposed or shared *by design*. However, the data scandals of 2018 saw the tech companies themselves come under fire for questionable privacy practices that were core to their very operation.

Among the big tech platforms, Facebook undoubtedly had the worst year, privacy-wise, in 2018. The company has been dogged by the bad press since the 2016 US presidential election when its role in the spread of disinformation and fake news came to light. Things went from bad to worse for the company when the Cambridge Analytica scandal, which revealed that the data of up to 87 million users had been harvested by the consulting firm without user consent, broke early in 2018.

In other words, 2018 was the year the public was confronted by the fact that the social media platforms they love to spend time on were using their personal data in ways many consider to be unethical, and that sharing user data in this way had been, in some cases, a component of the platform's business model.

Public concern is growing

These privacy snafus have not gone unnoticed by the general public, and survey data from 2018 suggests that they are having an impact on user behavior. A **survey from the Pew Research Center**, for example, shows that 42% of Facebook users said they "took a break" from the platform for several weeks or more at some point last year. In the same survey, 54% said they had updated their privacy settings. Elsewhere, **survey data indicate** that 3 out of 5 Americans have "very little or no trust" that social networks will protect their personal data.

Regulation is coming

The **General Data Protection Regulation (GDPR)** is a set of EU laws that was passed in 2016 and went into effect in May 2018. The regulation puts laws in place designed to protect the personal data and privacy of all EU citizens. Notably, the regulation affects all businesses that do business in the EU, regardless of where the company is based. Thus the GDPR is an EU regulation that nonetheless applies to U.S. (and all non-EU) companies doing business within the EU or with EU citizens.

However, stricter U.S.-based regulations that would apply to all American companies may also be on the horizon. The high-profile nature of the Cambridge Analytica scandal and others brought the issue of privacy to the attention of U.S. lawmakers. In December, a group of Democratic senators introduced a bill called the Data Care Act (DCA) which aims to stop the exploitation and misuse of consumer data. Senator Marco Rubio has also proposed his own bill, the American Data Dissemination Act (ADD). While it's not yet clear what data protection legislation in the U.S. will ultimately look like, it does seem very likely that it's imminent in some shape or form.

What businesses need to know

The high-profile privacy scandals that made headlines in 2018 may be in the rearview, but concerns about online privacy and user data protection are not issues that will fade with time. In fact, as more and more devices begin to come online and enter consumers' homes (think smart speakers and other connected devices), there is a significant risk that privacy issues will continue to proliferate.

Companies cannot afford to take security lightly. In order to avoid running afoul of existing and future legislation, and to do right by their users and customers, all online businesses need to make sure that they're investing first and foremost in protecting user data.

-
-
-
-
-