Privacy Is Suddenly a Financially Material Risk

By Tony Chapelle April 23, 2018

Boards at companies that depend heavily on personal consumer information are now on notice to either set up user-friendly privacy policies or lose customers and suffer regulatory and financial consequences.

Mark Zuckerberg's congressional hearings this month should have made it clear that U.S. privacy regulations are coming. Yet risk management experts say the immediate financially material risk is that some U.S. firms can't scramble fast enough to comply with Europe's stringent privacy protections. The General Data Protection Regulation, or GDPR, law takes effect on May 25.

At least 50% of companies that do business in Europe, including those from the U.S., won't be ready to comply by the end of this year, according to a 2017 report from technology research firm **Gartner**.

"In Europe," says board and management consultant **Diana Glassman**, "privacy is a treasured human right that's deeply rooted in [their] Nazi- and Communist-era history." European Union member states will doggedly enforce GDPR, says Glassman, founder of ESG financial consulting firm **Integration Strategy**. That's due to the collective memory of how totalitarians exploited sensitive religious, trade union or health information to round up and kill Europeans.

Indeed, many Commonwealth countries, including Canada and Australia, also have adopted similar rules. In all these countries, a consumer can ask to see her entire trove of personal information and have it deleted if she wants.

That's why Glassman says **Facebook**'s monthlong stock price fall in the wake of the **Cambridge Analytica** revelations "won't be just a buy-on-the-dip thing" this time. She predicts the same financial material risk that looms for Facebook will show up at other companies' doors when lax privacy practices are revealed.

"The fundamental [data-mining] business model of many tech companies is being challenged. It's unquestionable that people will reduce the amount of information they allow Facebook and others to use," says Glassman, a former **PwC** executive who developed privacy and data protection policies in 120 countries.

Verboten: Secret Tracking

GDPR even prohibits secret Internet cookies from tracking persons online unless those are strictly necessary for the user to receive an online service they requested. Sites won't be allowed to tell users they must accept cookies to enter. But a person may opt in to accept the text files.

Technology expert **Scott Relf** says that it's hard to grasp the size of the corporate ecosystem that uses harvested data. "Almost every big company in America is part of this since they buy online advertising. Chevrolet sells cars on Facebook. **Starbucks** advertises on Facebook," he says. "The entire marketing machine is intertwined with Mark Zuckerberg and Facebook."

A former product developer at **Procter & Gamble**, **Kellogg** and **Sprint**, Relf, with his wife, **Renée Relf**, now operates **PikMobile**, a new social network app that lets companies and individuals share photos and videos for $2 a month. He says paid services such as his represent the only alternative business model to mining consumers' data and sharing it with advertisers.

Behnam Dayanim, a partner at law firm **Paul Hastings** who co-chairs its privacy practice, writes in an e-mail that it's hard to know whether business models will change as a result of the GDPR. "Companies already were grappling with implications of the … GDPR for their ability to collect and monetize personal data. [At] companies that rely heavily on … sale or disclosure of data … I think internal compliance mechanisms will be tightened."

But Relf predicts that because of the European rule that consumers there must opt in to give companies permission to use their data — as opposed to the American model of having to opt out — Facebook and other ad-supported services such as Snapchat, **Twitter** and Google will soon be hunting for new revenue models. In the meantime, he expects the tech industry to accept more regulation.

The culmination of all this is financially material risk.

Equity analysts at **Deutsche Bank** estimate that once Facebook complies with GDPR provisions to allow European users to ditch being targeted for advertisers, 30% of Europe's users will opt out. The analysts forecast this will result in Facebook's having to reduce ad prices by 50%. That would cause a 4% slide in previous revenue estimates. The **U.S. Securities and Exchange Commission** on occasion has considered 5% a threshold for financial materiality in accounting.

Yet Glassman and investor Ridhi Kantelalpredict that most analysts underestimate how many consumers — not just in Europe, but around the world — will say no as online companies finally present them with clear, plain, easily accessible disclosures and consents.

Glassman and Kantelal see just 25% yearly revenue growth at Facebook in each of the next two years, versus other U.S.-based analysts' estimates of 35% to 40%. That's because Facebook cash flow in fiscal year 2018 will grow substantially slower than the 50% hike between 2016 and 2017, Kantelal claims. And while most

analysts forecast 2018 earnings per share increases of 35% to 65%, Kantelal says it will be just 20%.

Russell McGuire, a senior practice leader at Origami Risk, a technology management consulting firm, observes that some U.S. corporate leaders are almost in a state of denial about GDPR.

He describes making several risk management presentations in the last 18 months at U.S. companies with customers and operations in Europe. “They’re capturing credit card information from consumers; they have data on customer product warranties. But when I tell them about risks from the GDPR, often the response is, ‘That’s a European law; we don’t have to bother with it.’”

But that’s incorrect, McGuire explains. “They must have the same privacy controls as Europeans. And there’s not much time.” Indeed, Zuckerberg told senators in his hearing on Capitol Hill that, where local laws allow, he’s going to step up Facebook’s privacy standards in every country to the same level required in Europe.

Of course, the largest penalty for breaching GDPR is 4% of annual global sales or €20 million, whichever is higher. That maximum fine would be imposed for the most serious infringements, such as not having customer permission to access personal data or violating the so-called Privacy by Design concepts.

There’s also a GDPR requirement to enter into a sunset agreement with each EU resident and set a date for when their data will be deleted.

In London, **Gareth Thomas**, director of data privacy for U.K.-based governance consulting firm GoodCorporation, says the GDPR’s maximum 4% fine will likely be used against companies that deliberately flout privacy regulations. Thomas, a former investment banker at **CIBC World Markets**, envisions that the EU might slap it on bad-boy tech companies that believe it’s better to ask for forgiveness after breaking regulations than to ask for permission before. Also, the EU probably would throw the whole book at firms whose abuse had very damaging or widespread impact on the public.

McGuire advises boards to tell management to report on how far along the road to GDPR compliance their company is now. The report should also point out how and when the enterprise will achieve 100% acceptable status under GDPR.

“Have that recorded in board minutes, and it then needs to be backed up by action, such as being verified by the auditors as being in place,” he says.

If there were any legal actions against the company, prosecutors would want to know if the board had been aware whether policies had or had not been improved. If they hadn’t, the board would be in a very weak position to respond to claims against them.

Thomas, the privacy expert in Britain, says corporate leaders there ultimately admit that the new privacy law makes for better governance.

“I was talking to the general counsel of a very large telco [in the U.K.] about GDPR. And she paused and said that [her executives] had realized that GDPR is just a best practice for treating customer information [respectfully],” he says.
“You would have never heard that five years ago from a general counsel.”