Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 30, ISSUE 9 / OCTOBER 5, 2012

WHAT'S INSIDE

FOIA

News editors, blogs ask Supreme Court to rule on state FOIA laws

Several organizations representing newspapers and Internet news platforms have asked the U.S. Supreme Court to resolve discrepancies between states' freedom-of-information laws so that out-of-state news organizations can access state-controlled public information.

McBurney et al. v. Young et al., No. 12-17, amicus brief filed (U.S. Aug. 28, 2012).

The Supreme Court should grant the writ of *certiorari* petition that Mark J. McBurney and Roger W. Hurlbert filed after a federal appeals court ruled that Virginia may grant access to its public records to state citizens only and may deny access to out-of-state applicants, such as journalists and bloggers, the *amicus curiae* brief says.

In February the 4th U.S. Circuit Court of Appeals said the "citizens only" provision of the Virginia Freedom of Information Act, Va. Code Ann. § 2.2-3704(A), did not violate the U.S. Constitution's "privilege and immunities" or "dormant commerce" clauses.

McBurney and Hurlbert appealed to the Supreme Court to reverse that decision, and the news advocacy groups, blogging platforms and websites agree.

Blogging platform Tumblr was among the organizations that filed the amicus curiae brief.

The *amicus* brief was filed by the American Society of News Editors, technology news website Ars Technica, left-leaning political blog Daily Kos, and blogging platforms Tumblr and WordPress.

"Journalists rely on state FOIA requests to break news stories of national significance," the brief explains. "Yet journalists continue to face

CONTINUED ON PAGE 6

COMMENTARY

Practical responses to data privacy developments in the United States and the European Union (Part II)

In the second of this two-part series, Robinson Bradshaw & Hinson attorneys John M. Conley and Robert M. Bryan discuss the European Union's draft regulation on privacy and what it means for companies that do business in Europe. They compare the EU's preference for a top-down approach — enacting laws that dictate compliance — with the "recommendations" that the Federal Trade Commission provides in its March 26 privacy report.

SEE PAGE 3

41247083

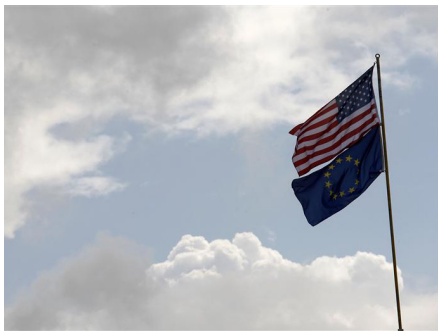
Practical responses to data privacy developments in the United States and the European Union (Part II)

By John M. Conley, Esq., and Robert M. Bryan, Esq.
Robinson Bradshaw & Hinson

It is useful to compare the Federal Trade Commission's recent activities with parallel developments in the European Union. On Jan. 25 the European Commission[1] released a long-awaited Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.[2] As it usually does, the EU has chosen an aggressive regulatory approach, eschewing recommendations of "best practices" in favor of a top-down legal mandate. If the regulation receives final approval from the EU Parliament (a process likely to take two years or more) any company that collects or processes the personal data of EU citizens and that is subject to personal jurisdiction in the EU will have to meet a series of onerous requirements. They include obtaining the subject's affirmative consent, providing notice of the purposes of the data collection and, most controversially, offering a broad "right to be forgotten."

DRAFT REGULATION

It is significant that the commission is acting by *regulation* rather than *directive*, as was the case with the current privacy law, which was enacted by directive in 1995. Once it receives final approval, a regulation takes effect uniformly throughout the EU, whereas a directive is adopted on a country-by-country basis. The regulation approach has two significant implications. First, it means the new rules will take effect simultaneously throughout the EU rather than awaiting adoption by individual national governments. Second, there will be no room for country-by-country variation in implementation, as is sometimes the case with directives.



REUTERS/Tobias Schwarz

As it usually does, the EU has chosen an aggressive regulatory approach, eschewing recommending "best practices" in favor of a top-down legal mandate.

The portions of the regulation that deal with the scope of its application take a very aggressive approach to the EU's authority to regulate and impose penalties on U.S. and other foreign companies that do business in Europe. The regulation will cover all data-processing activities (very broadly defined to include any kind of operation — automated or not — that might be performed on data that is reasonably identifiable to an individual) by companies inside or outside the EU that are engaged in "offering goods or services" to people in the EU or "monitoring their behavior." This language suggests that the EU intends to apply the regulation to the limits allowed by international norms of personal jurisdiction, which require that the company have "minimum contacts" with an EU country.

The draft regulation allows an EU resident to bring a private enforcement lawsuit in a national court of the country where the plaintiff resides or the defendant has a business establishment. In addition, EU authorities can impose substantial administrative sanctions on violators. The sanctions are specifically required to be "effective, proportionate and dissuasive." Penalties will vary depending on the nature of the violation, but they can range up to €1 million or 2 percent of the violator's worldwide turnover. These remedies go substantially beyond what is available under federal or state law in the United States. In the United States, as we described in Part I, the FTC may bring an enforcement action against a company that fails to provide

John M. Conley (L) is of counsel at **Robinson Bradshaw & Hinson** in Charlotte and in Chapel Hill, N.C. His practice focuses on intellectual property and privacy, and he has published and spoken widely on these topics as well as the social scientific study of law and finance. Conley, who also is the William Rand Kenan Jr. professor of law at the University of North Carolina at Chapel Hill, can be reached at JConley@rbh.com. **Robert M. Bryan** (R) practices in the firm's Charlotte office, where he covers a broad range of intellectual-property-intensive acquisitions, joint ventures, licenses and other commercial transactions. He can be reached at BBryan@rbh.com.

reasonable privacy or security protections, but penalties have rarely approached the levels that the EU draft regulation provides. Moreover, private lawsuits in the United States almost never succeed unless the plaintiff has suffered financial loss as a result of identity theft.

> The portions of the regulation that deal with the scope of its application take a very aggressive approach to the EU's authority to regulate and impose penalties on U.S. and other foreign companies that do business in Europe.

Individuals or "data subjects," also broadly defined to include anyone who can reasonably be identified from the date in question, will have significantly more rights than under current EU law. For example, a company will have the burden of proving that every subject has given consent for the processing of their data for specified purposes. The law defines consent as "any freely given specific, informed and *explicit* [emphasis added] indication of will," and it says consent can be withdrawn at any time. The subject will also have a "right to be forgotten, and to erasure." This means that when the subject withdraws consent or "the data are no longer necessary" for the purposes for which they were collected, the company must render the data inaccessible, including on the Internet.

This requirement will be problematic for U.S. companies for at least two reasons: It is likely to come into conflict with American First Amendment principles and, on a practical level, it will be extremely difficult, if not impossible, to implement. On the first point, any law requiring companies to erase Internet content, especially if the subject is a matter of public interest, would be vulnerable to a First Amendment challenge. Second, how would it be done on a practical level? Just how would a company go about ensuring "erasure" of Internet content?

The draft regulation also requires companies to adopt policies and procedures that ensure adequate data security and to provide prompt notice of security breaches. For the most part, these requirements should be met by adopting "best practices" as that term is understood in the United States — that is, doing at least as much as most of the companies in a particular industry and following agreed-upon industry-wide guidelines, if available. However, there is a possibility of inconsistency because the law also authorizes the EU Commission to establish the "state of the art" for data security by further regulation. Thus, companies using best practices, as understood in the United States, may suddenly be confronted with a new state of the art as defined by EU regulators. This provision will also increase the administrative burden for data breaches by adding the requirement of reporting any breach to an EU supervisory authority, generally within one day.

EXISTING EU LAW

Even as the draft regulation starts to make its way through the parliamentary process, a variety of EU privacy officials have been pushing for a stricter interpretation of privacy rights under existing EU law. In a letter released in March the Article 29 Working Party, an EU-sponsored organization that addresses privacy issues, criticized a proposal from an advertising trade association to implement Do Not Track via a link to a comprehensive website and argued instead for a browser-based protocol.[3] The advertisers favor an approach that relies on an icon and link within ads that would connect users to a website that would inform them of their rights. The Working Party, in contrast, has been calling for a one-stop DNT setting in a consumer's browser. At the same time, the EU's commissioner for digital agenda criticized companies for not obtaining sufficiently explicit consent from users before installing cookies on their computers — even while acknowledging that "there are different interpretations, sometimes, or even confusion about what the rules mean and how to comply with them."[4] And lest anyone think that all this is just a European issue, the chairman of the Article 29 Working Party, while on a tour of Silicon Valley, said "enforcement actions ... will be taken" against non-compliant U.S. companies.[5]

A final piece of the puzzle is the continuing impact of a 1995 EU directive that forbids the transfer of personal data about EU citizens to countries, including the United States, that do not provide an EU level of privacy protection.[6] Even intra-company transfers are affected. The present options for U.S. companies include joining a Department of Commerce "safe harbor" program under which companies must demonstrate an adequate privacy policy; conducting data transfers under EU-approved standard contractual clauses, which many U.S. companies find too onerous; and adopting EU-approved, legally effective binding corporate rules, which also have been unpopular in this country. As EU data requirements become even stricter, and with the United States likely to remain on the EU's disapproved list, staying eligible to engage in U.S.–EU data transfers can only become even more difficult.

LOOKING AHEAD

These legal developments on both sides of the Atlantic pose a series of practical questions. For instance, for those companies that do business (especially electronic business) internationally, are there efficient ways to prepare simultaneously to follow the FTC's framework and prepare for coming changes in EU law?

3 steps for U.S.-based international companies to take now while planning for the future

1. Carefully assess internal data polices to understand exactly what personal data it collects and how it is storing and using this data.
2. Match current data collection practices with actual business needs, and develop and implement uniform, documented policies that ensure that the company is collecting and retaining only personal data that is actually needed.
3. Make sure that data security measures meet generally accepted best practices by U.S. standards.

The EU draft regulation moves Europe, predictably, in the direction of tighter top-down regulation. In a technical environment that offers ever-expanding and increasingly sophisticated ways to collect and use personal data, the EU wants companies to head in the opposite direction by limiting the data they may collect and use, and by developing the ability to respond to inquiries and demands from individual EU residents who want to limit how those data are used. The potential penalties will include not only substantial fines but also prohibition of foreign companies from engaging in data transactions with EU companies and consumers. Most observers think the final adoption of the draft regulation is at least two years in the future. However, the potential changes are so sweeping, and the potential costs of non-compliance are so severe that affected U.S. companies should not wait until the last minute to develop a plan.

more regulatory and far less flexible than any standards that the FTC is likely to develop.

With regard to the first point: there is probably little or nothing that a U.S. company should do to prepare for the right to be forgotten. Since advocates of free speech and freedom of information in the EU are trying to force significant changes before the draft regulation is finalized, attempts to meet the onerous burden of compliance in advance (*e.g.*, by setting up "technical measures" to provide erasure on request and notify third-party publishers) are probably premature. At the moment, the most sensible approach seems to be to wait and see what happens in the EU.

On the second point, though, much can be accomplished. One way to look at the draft regulation is as a more aggressive version of the final report; Conversely, the final report can be seen as the "draft regulation lite."

> The draft regulation also requires companies to adopt policies and procedures that ensure adequate data security and to provide prompt notice of security breaches.

EU REGULATION VS. FRAMEWORK OF THE FTC FINAL REPORT

It is probably no coincidence that the general principles of the framework of the FTC final report (policy transparency, data security and accuracy, consumer choice and control [particularly in the area of tracking] and limits on third-party transfer) are conceptually similar to those articulated five months earlier in the EU draft regulation. In fact, they are principles that have been discussed for years by the global privacy community.

Nonetheless, there are two major differences.

First, the major policy innovation of the draft regulation — the right to be forgotten — is all but inconceivable in the United States for reasons having to do with both First Amendment law and free-speech traditions. Second, from an overall perspective, the EU's approach will be, as it invariably is, far

What this means is that every step toward compliance with the FTC's framework will also be a step toward compliance with the EU's regulatory regime. Doing business in the EU may ultimately require more, but in many important respects it will be more of the same.

With this in mind, there are at least three specific steps that any affected U.S. company should be taking now to prepare for the coming changes both at home and abroad. First, each company should carefully assess its internal data polices to ensure that it understands exactly what personal data it is collecting and how it is storing and using that data. In doing so, it must bear in mind that the EU's draft regulation broadly applies to *any* information relating to an identified or reasonably identifiable natural person, whether it is in electronic form or written files.

Second, each company should match its current data collection practices with its actual business needs, and develop and implement uniform, documented policies that ensure that it is collecting and retaining only personal data that are actually needed.

Finally, each company should ensure that it is using generally accepted best practices, by U.S. standards, in the way that it provides data security. All of these steps have multiple advantages. From a practical perspective, they improve the quality of a company's data-handling and, from a legal point of view, they start the process of preparing for both the incremental changes underway in the United States and the more dramatic changes coming in the EU. WJ

NOTES

[1] The European Commission is the EU's executive branch that comprises, as in the United States, many regulatory agencies, but it lacks a powerful, United States-style chief executive.

[2] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), EU: COM (2012) 11 (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[3] *See* Jennifer Baker, *European Watchdog Pushes for Do Not Track Protocol*, PCWorld (Mar. 6, 2012), *available at* http://www.pcworld.com/businesscenter/article/251373/european_watchdog_pushes_for_do_not_track_protocol.html.

[4] *Id.*

[5] Martin Kaste, *Europe Pressures U.S. Tech On Internet Privacy Laws,* NPR Online (Apr. 30, 2012), *available at* http://www.npr.org/2012/04/30/151688976/europe-pressures-u-s-tech-on-internet-privacy-laws.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, EU: Directive 95/46/EC (Nov. 23, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.