Case #11b. Ad Tech Firms and Publishers versus European Privacy Law

(edited)

By Jack Marshall Dec. 16, 2015 Wall Street Journal

A new European digital privacy law, the *"General Data Protection Regulation (GDPR,"* supported by **European privacy advocates (EPA)** could have serious consequences for online advertising in the region, threatening everyone from ad tech middlemen to publishers to Web giants like Google and Facebook, industry executives say.

European Union officials, led by the **European Commission**, reached agreement Tuesday on the pan-European law, creating a strict new legal framework that dictates how companies can use individuals' personal information. The law requires approval from the EU Parliament and European governments.

The new rules could limit the ability for companies to collect and process online data, a practice on which many business-to-business online advertising companies currently rely. Such companies include Google, Yahoo, Criteo, AOL, Rubicon Project, OpenX and many others.

The changes could also impact publishers -- from well-known news providers to smaller ad-supported sites -- who buy services and technologies from online ad vendors to help them deliver targeted ads to their readers and otherwise generate revenues from their audiences.

Townsend Feehan, chief executive of the **European unit of the Interactive Advertising Bureau (EIAB)**, an online advertising trade group, described the new law as "a setback" for Europe's digital economy.

"There's not yet a clear understanding of what of the consequences will be, but it could mean there are fewer options for publishers in terms of monetization," Ms. Feehan said. "The transition to digital for publishers has already been troubling, so to threaten the business model on which they rely seems counterproductive."

Data-driven advertising now forms the backbone of the $59 billion global online ad industry, and hundreds of companies have emerged in the past 20 years offering various services and technologies related to it.

Online data collection allows marketers to target ads to specific types of users, and to measure and analyze the results of their campaigns. The practice also helps publishers generate advertising revenue from their digital audiences.

According to Ms. Feehan, her primary concern centers on the concept of user consent as it relates to the collection and processing of data. The new laws could result in companies having to gain more explicit consent from consumers for those practices, which could be difficult for third-party companies which don't have a direct relationship with consumers.

For example, a publisher may not be able to use a third-party advertising network to target ads to a user of its website if that third-party does not have permission from the user to do so. Many publishers now work with dozens of different ad networks and ad tech companies to help them generate revenue from their visitors.

"B-to-B companies may have a seriously reduced scope," Ms. Feehan said, while large platforms operated by companies such as Facebook and Google may find themselves at an advantage since they have a direct relationship with consumers in many instances.

Google and Facebook declined to comment.

That said, those companies also operate as third-parties in many instances, Ms. Feehan pointed out. They help to sell, target, track and measure ads on properties owned by other companies.

"This is awkward for them, too," she said.

EU Data-Privacy Law Raises Daunting Prospects for U.S. Companies

Sweeping digital-privacy regime runs counter to practices that have become commonplace in the U.S.

By Elizabeth Dwoskin Wall Street Journal

(excerpt)

The sweeping new digital-privacy regime that European Union officials agreed to on Tuesday, the*"General Data Protection Regulation (GDPR,"* runs counter to practices that have become commonplace in the U.S., according to several American corporations.

The combination of stiff penalties and ambiguously worded provisions in the new EU-wide data-protection law, which would replace a patchwork of 28 national laws, raises daunting prospects for companies operating in Europe.

U.S. companies in industries ranging from advertising to health-care have embraced the opportunity to analyze vast amounts of data collected from sensors, apps and other sources. The

new law places substantial roadblocks in their way, companies say, by specifically targeting data mining and user profiling.

Executives from some Silicon Valley corporations say that the new law poses a big threat because it combines legal uncertainty with massive fines of up to 4% of global revenues. Some provisions rely on fluid notions, like risk-based harm to individuals, that could be interpreted differently by companies and regulators.

"Legal uncertainty and big fines are a toxic cocktail," Allan Sørensen, a board member for **EIAB, an advertising trade group** that advocates for **ATFP**.

One provision appears to challenge what companies call "secondary uses" of personal data beyond the purpose for which it was collected. For instance, a weather app may collects location data to offer localized forecasts and then use the data to display a targeted ad.

U.S. consumers typically consent to such uses by checking a box next to a blanket privacy policy that covers all possible uses of data. The new European regulations could require specific consent for each use, said Martin Abrams, executive director of the **Information Accountability Foundation (IAF),** a think tank that is supported by technology companies.

It may be impossible to gain consent for every possible use of data, said Hilary Wandall, Chief Privacy Officer for pharmaceutical giant Merck & Co. Inc. Such consent is particularly challenging with respect to medical databases in which some individuals are deceased, she said.

The new law is expected to include tighter rules on a practice called "profiling," or sorting users into buckets based on their online behavior. For instance, insurers use sensors attached to cars to price their premiums, and social networks use face detection technology to identify individuals in their users' photographs.

The law gives users the right to know why they are being profiled, what buckets they are sorted into, who receives the data, the logic involved in drawing conclusions and "the consequences of such processing."

Companies typically disclose to consumers that they may target them with an ad based on their information or behavior, but rarely disclose the categories they are sorted into.

"Right now, so much of our online lives are determined by algorithms that are totally opaque, said Alvaro Bedoya, executive director of the **Center on Privacy and Technology** at Georgetown University Law Center. "The right to access the 'logic' behind data processing could be a significant step forward in opening that black box."

He pointed out that the law carves out exceptions to protect trade secrets, intellectual property, and anonymized data used for research purposes.

The new law also enshrines a broader version of the controversial "right to be forgotten," applied to search engines since a 2014 decision by the EU's top court. The new version requires any

company to delete personal information it has about individuals who request that it be removed, except in certain circumstances, such as when that information is necessary for historical research or for exercising free expression. Search engines including Alphabet Inc. 's Google said the rule has already proven difficult to comply with.

Barbara Mangan, eBay Inc. 's privacy counsel for North America, said the company had been working for two years to find ways to fulfill European requests to have their data deleted right away. The solution was complex because a customer's data might be held in dozens of databases at any given time.

European Parliament and EU governments still need to approve the law, which is considered likely, after which it would take effect in two years.

The EU Data-Privacy Agreement: What We Know and Don't

- By Jacob Gershman, Wall Street Journal

European Union officials have struck an agreement to replace a patchwork of national privacy laws with a EU-wide legal framework for data sharing and collection.

Companies and legal experts are still absorbing the more than 200-page rule package called the *"General Data Protection Regulation (GDPR)."* The final agreement, if approved by the **European Parliament** and the **European Council**, won't come into force for at least two years.

Here's a snapshot of what we know and don't.

Expanded scope: Here are some comments:"It won't take much to fall under the GDPR's reach, because the jurisdiction is defined digitally, not physically.

The regulations cover "online activities of non-EU companies that offer goods or services to, or monitor the behavior of, EU individuals." That could "apply to virtually any business that offers its products and services in the EU market

New individual rights: The rules create or clarify rights for people to control their personal data. Among them:

• Tougher consent requirements: To use their data, businesses have to get consent from users, defined as "freely given, specific, informed and unambiguous indication of his or her wishes." The draft rules say "silence, pre-ticked boxes or inactivity" doesn't count. The rules set a stricter standard of "explicit" consent for more sensitive data, such as information "revealing racial or ethnic origin."

• The rules also boost the digital age of consent to 16 years old from 13. Companies wouldn't be allowed to collect data from children younger than 16 without parental permission. A U.S. tech executive told WSJ that if the rule is enforced, it could lead companies to stop offering services to kids under 16.

• A broader right to be forgotten: Last year the European Court of Justice recognized the right of individuals to remove Internet content about them deemed "inadequate, irrelevant, excessive or outdated" with some exceptions. The EU wants that right expanded. According to the daily online newspaper EUobserver:

The new rules seem to involve broader justification. According to the commission's description, "when you no longer want your data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted."

• The right to know when you've been hacked: Companies would be required to tell regulators about a personal data breach "not later than 72 hours after having become aware of it." Notification wouldn't required if the breach is "unlikely to result in a risk for the rights and freedoms of individual."

Higher fines: Administrative fines for non-compliance could be as high as 4% of a company's world-wide revenue.

More centralized enforcement: EU officials says the regulations will allow business to deal primarily with a single national privacy regulator within Europe. It's not quite a "one-stop-shop," the term used by EU officials. A company can be dealing with an authority based in one country, but when dealing with big companies that operate in multiple EU countries, other authorities in different member states can review rulings and take the matter to a pan-European board of regulators.

The big unknowns: There are many but one is how aggressively the rules would be enforced given their sweep. The potential conflicts with U.S. data laws is a looming question, he said. Tensions could come up in situations when a U.S. court or regulator requires a company covered by the EU law to turn over information about an EU citizen, he said.

The rules, "will require a massive amount of analysis and adjustment for many organizations, keeping privacy professionals, legal departments and outside counsel busy for a long time."

EU Officials Reach Agreement on Text of New Privacy Law

Deal on EU privacy law caps four years of haggling, lobbying

By Sam Schechner Dec. 15, 2015 Wall Street Journal

European Union officials reached agreement Tuesday on a pan-European digital-privacy law, creating a strict new legal framework that will have ripple effects globally on how companies can use individuals' personal information.

After nearly four years of haggling and lobbying, negotiators agreed late Tuesday on a final text of the EU-wide bill, which will replace a patchwork of 28 different sets of national privacy laws, and boost the bloc's paltry privacy penalties to potentially billions of euros, EU officials said.

Under the agreed text, fines would rise to a maximum of 4% of a company's world-wide revenue, the officials added.

The text, which must be definitively approved by the **European Parliament** and **EU governments acting through the European Council** before going into effect in two years' time, is expected to tighten rules for getting online consent and create new responsibilities for cloud-services companies.

EU officials say the new law will lighten the administrative burden for companies, by allowing them to deal primarily with a single national privacy regulator that will allow them to operate across the entire EU. They also say that by creating a high privacy standard for firms operating in Europe, the continent can help create an environment where pro-privacy business models grow, becoming an advantage for individuals, for firms and for the region.

"The new rules will give businesses legal certainty by creating one common data protection standard across Europe," said Jan Philipp Albrecht, a member of European Parliament who participated in the negotiations, adding that the rules "will give users back the right to decide [about] their own private data."

Moreover, newer data-mining practices could be curtailed because companies may have to seek additional consent from users every time they want to reanalyze or re-purpose their data. A privacy policy in which a user simply checks a box and signs off on all uses of their data won't be sufficient, said Martin Abrams, executive director of the Information Accountability Foundation, a think tank that is supported by technology companies.

Online advertising and data-analytics companies say their businesses could be hit. The new law is expected to include tighter rules on a practice dubbed "profiling," which could complicate life for data-hungry brokerages and exchanges that use large pools of personal information including online browsing histories to tailor automated online offers to individuals.

The new law also includes potentially higher bars for requiring user consent across the online-advertising value chain. "The way it works now probably won't be legal" in some cases, said one executive for an online-advertising measurement business. "It could potentially stop some interest-based online advertising models."

The negotiations that ended Tuesday were between representatives of the **EU Parliament**, **EU governments** and the **European Commission**, the bloc's executive. Agreements reached in such negotiations are usually adopted without further amendment.

Question

What strategy do you recommend for the Ad Tech Firms and Publishers (ATFP) to achieve its goal of stopping the imposition of Europe's proposed *"General Data Protection Regulation (GDPR)"* in the EU Parliament, EU Council, and/or the EU governments?

In answering this question, you must first:

a) **(6) draw a power diagram showing relations among the primary actors in the case. (They are those highlighted in the case).**
b) **(3) Define what model will best describe the public policy decision-making of each of the governmental actors in this case and explain your choice: (1) the EU Parliament, (2) EU Council, and/or (3) the EU governments (You must view each of these governmental actors separately, even if you conclude the same model applies to all three. Also, you may assume the same model applies for each of the 28 EU country governments!) (40 words maximum for each government actor)**
c) **(5) In formulating your strategy, given your power diagram and the models you have cited, be sure you make clear what power has ATEP (and its potential allies) over the government decision makers and other actors. (200 words maximum)**

Summary of Actors in the Case

Ad Tech Firms and Publishers (ATFP)

European Commission (EComm), the executive branch of the EU

EU Parliament (EUP)

EU governments (EUG)

European Council (ECou) made up of the heads of the 28 EU states

European unit of the Interactive Advertising Bureau (EIAB)

Information Accountability Foundation (IAF)

Center on Privacy and Technology (CPT)

European privacy advocates (EPA)