collective wisdom®

SZABO ASSOCIATES, INC. VOLUME 34, ISSUE 1, MARCH 31, 2019

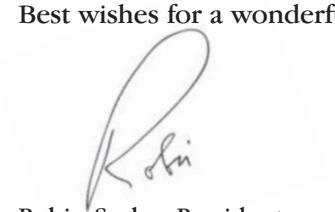
MORE is better than less.

Dear Friends:

Data privacy has been in the news a lot lately, giving many of us pause about just who knows what personal information about us and what they might do with it. If the U.S. has historically been a bit more relaxed in our approach to privacy, the European Union has not. Believing that privacy is a fundamental human right, the EU last May put into effect its "General Data Protection Regulation," or GDPR, the most sweeping data privacy regulation in 20 years. This issue will explain what the law requires, how it affects U.S. media companies, and what we can expect this year regarding legislation in our own country.

We announce with pleasure that longtime associate Randy Neff has been named Vice President of Szabo. Also, we look forward to the MFM/BCCA 59th annual conference, "Media Finance Focus 2019," May 19-22, at the Hilton New Orleans Riverside, New Orleans, LA. Szabo is pleased to sponsor the opening night party at B.B. King's!

Best wishes for a wonderful spring,



Robin Szabo, President
Szabo Associates, Inc.

GDPR . . .

Some Pain, Some Gain for Media

Is privacy a fundamental human right? If you ask the European Union, the answer is "yes." As of May 25, 2018, the EU requires all companies that collect, use, and share data about EU residents to adhere to its new data privacy and security measures, "General Data Protection Regulation," or "GDPR." Failure to do so can result in severe penalties, as high as four percent of annual global revenue, regardless of whether the organization is located within the EU or not.

Why It Matters.
You may be thinking, "Why should we, a U.S. company, care about a European law that applies only to its own citizens?

Any U.S. company that has a Web presence and that markets over the Web needs to pay attention to GDPR, according to Yaki Faitelson, CEO of data security and analytics firm Varonis and Forbes Council member, in his post, "Yes, The GDPR Will Affect Your U.S.-Based Business." If you collect personal or behavioral data about a citizen in an EU country, you are subject to its requirements. The word "in" is an important distinction, states Faitelson. The subject must be in the EU when the data is collected. Otherwise, the law does not apply.

Money does not have to change hands to fall under the scope of the law. If your organization targets EU citizens and collects their personal data for marketing purposes, the data must be protected according to GDPR, said Faitelson. Marketing in an EU country's language and accepting its currency would certainly constitute "targeting."

GDPR broadens the definition of personal data to include virtually any information about a person. Information that relates to an identified or identifiable natural person (data subject) falls within the definition of Personal Identifiable Information (PII), including information that enables a company to identify, contact, or locate a person, even if that process is indirect. Certain types of data are considered more sensitive and therefore come under greater scrutiny than others, including financial/credit, health/medical, genetic/biometric, ethnic origin, political opinion, religious/philosophical, and sex or sexual orientation.

The law imposes higher standards for establishing "valid consent." Consent to use personal data must be "freely given, specific, informed, and unambiguous" and made by a statement or by a "clear affirmative action." The data may be collected only for a "specific purpose" and may not be used for any new, incompatible purposes. Additionally, EU citizens may require companies to erase their personal data at any time if they choose to withdraw consent.

Because the individual "owns" the data, the law requires service providers such as Facebook and Google to make the data they hold on individuals portable, allowing an individual to take it to a competing service. In his article, "How GDPR Will Transform Digital Marketing" in the *Harvard Business Review,* Dipayan Ghosh, Fellow at New America and the Harvard Kennedy

—continued on page 2

GDPR —

—continued from page 1

School, argues that this requirement, barring the construction of some loophole, weakens the incentive to collect the data in the first place.

It should be noted that publishers can continue to use data that is aggregated and anonymized for every purpose from analytics to ad targeting, continue to conduct their own marketing activities (as long as they give users an easy way to opt out), and continue to collect data for other purposes, such as ensuring that readers are subscribers and to craft and deliver relevant content.

The Implications.

Let us assume your company's marketing efforts include the collection of PII from EU citizens. What does the GDPR expect you to do about it? It is all about consent, data protection, and accountability.

Consent. Your EU data subjects must actively agree to the collection of personal data. Requiring the consumer to check a box indicating agreement to your Terms and Conditions does not meet the GDPR consent regulations. Agreement must not be by default. In other words, you cannot pre-check a consent box and require the consumer to "un-check" it to refuse consent. Additionally, you must explain how you intend to use the data in clear language. If there are multiple uses, each one requires active consent.

Cookies get a brief mention in the GDPR; however, the law provides a significant update. The EU has made it clear that, if a site uses cookies, it is collecting personal data, requiring a robust opt-in consent. As a result, the site must abandon its use of cookies or obtain consent from customers.

Data protection. GDPR demands accountability. Companies must be able to demonstrate compliance through data protection impact assessments and other mandatory internal procedures. Also, international transfers of personal data outside the EU require additional precautions.

Another significant GDPR rule that may cause a collective IT headache involves breach notification. A breach involving "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" must be analyzed to determine whether the exposed or affected personal data identifiers can cause "risk to the rights and freedoms" of EU data subjects. According to Faitelson, the GDPR gives some leeway in weighing the risks, but a large exposure of email addresses, sensitive data related to medical or financial information, or identifiers associated with children would all require notification to an EU regulator or "supervising authority" within 72 hours. Additionally, a breach that causes "high risk" to fundamental property rights, such as credit card numbers or account passwords, requires notification to the subjects themselves.

Present Risk.

Significant enforcement activity and new laws have been enacted or proposed since the start of 2019, indicating that regulators in the EU and the U.S., several U.S. states, and the Congress mean business with regard to data privacy. In their February 27 contributing post to global law firm Norton Rose Fulbright's *Data Protection Report,* Jeewon Kim Serrato and Daniel Rosenzweig provided an overview of recent enforcement actions, changes in the U.S. landscape, and Congressional consideration of new federal laws.

The French data watchdog CNIL used its powers under GDPR to levy a $56.8 million fine on Google, stating that the search-engine giant violated rules requiring information about data collection to be transparent and users to be sufficiently informed. *The Washington Post* reported on February 14 that the FTC is currently negotiating a multi-billion dollar fine against Facebook to settle the agency's investigation into its privacy practices. According to Serrato and Rosenzweig, these CNIL and FTC actions signal that data privacy enforcement risk is now one of the top risks a company must consider as part of its enterprise risk management framework.

Several U.S. states are now proposing their own data protection laws that provide certain GDPR-like consumer rights; however, say Serrato and Rosenzweig, the U.S. states' approaches have key differences noteworthy for businesses operating in the U.S. California has forged ahead with its California Consumer Privacy Act (CCPA), passed last June and set to go into effect on January 1, 2020. Not to be outdone, a total of 11 states introduced similar legislation, which include slightly different regulations than both the GDPR and CCPA. Serrato and Rosenzweig opine that these laws would exact significant costs to businesses trying to create a privacy framework to accommodate these overlapping and conflicting requirements.

The legal complexity and uncertainty posed by these changes are leading businesses to call on Congress to implement national comprehensive data privacy legislation, which would represent a first-ever federal privacy standard. The House Energy and Commerce Committee and the Senate Commerce Committee are presently holding hearings on key issues that need to be addressed.

The Good.

What is described here is intimidating, to say the least. Is there anything about GDPR that can benefit media publishers?

Advertiser/media relationships. In his September 2018 article for *Media Post Publisher's Daily,* Casey Wuestefeld, VP of Campaign Operations at Nativo, stated that one truth had emerged within the first few months since GDPR went into effect: "Advertisers' relationships with publishers are more important today than they've ever been." Brands that have relied on third-party data, says Wuestefeld, have felt the pinch of GDPR more than others. While first-party data has always been an important asset for brands, its importance has become even greater since the law went into effect. Wuestefeld cites two trends in the post-GDPR world—the reemergence of contextual targeting and the rise of second-party data from publishers.

Contextual advertising is nothing new; however, it has become more sophisticated over time. No longer is it merely placing ads in a publication whose audience demographics align with the advertiser's.

Machine learning and artificial intelligence (AI) have taken placement-level contextual targeting, such as sponsored content and native advertising, to a new level. And no one, according to Wuestefeld, has better data than the publisher for driving the most relevant placements.

The rise of second-party data does put publishers in the hot seat for obtaining consumer consent to capture and use their data. On the other hand, the direct relationships they share make consent more likely, and the result will be more valuable than third-party data. Advertisers can subsequently, in a GDPR-compliant way, reach out to these consumers to establish direct relationships.

As far as cookies are concerned, their loss may prove to be beneficial to both consumers (who dislike them) and advertisers (who embraced them). Forbes Agency Council member Susan Akbarpour, CEO of Mavatar Technologies, in her article "How Does GDPR Impact Advertising and E-Commerce," stated that many programmatic advertising technology providers, ad and affiliate networks are "clinging to phony marketing metrics like cost per click (CPC), click-through rates, cost per thousand (CPM) and more—all of which rely on cookies." Akbarpour believes that user-generated advertising, such as influencer marketing or sponsored content on consumer-facing sites, has the potential to grow exponentially in our post-GDPR world. A self-described blockchain enthusiast, she also suggests that blockchain promises to disrupt antiquated attribution models, remove bad actors and middlemen, and increase transparency, security, and profitability to advertisers.

Advertiser/consumer relationships. Akbarpour has plenty of company in the blockchain fan club. As reported by Melynda Fuller in her February 26 article for Media Post, a new study, the "Blockchain MarTech Landscape," released by Brave Software and Never Stop Marketing Research, revealed that blockchain-based solutions for marketers enjoyed an uptick of 1218% in just 18 months. On the same day, Brave, creator of a privacy browser and blockchain-based digital advertising platform, announced a new blockchain-based solution to connect consumers with more than 250,000 brands through a partnership with rewards platform TAP Network, home to brands such as Paramount Pictures and Red Bull. The partnership allows users who watch opt-in private ads from Brave's brand partners to exchange their earned Basic Attention Tokens (BAT) for real-world rewards. Clearly, this is the era of consumers, who have high expectations of the brands with which they choose to associate. The general wisdom today is that brands that refuse to address consumer expectations, including data usage and rewards for their loyalty, will be left in the dust.

For Now.

Because the GDPR, CCPA, and other state and U.S. legislative proposals each introduces new and different requirements on the collecting, processing, sharing, and maintaining of personal data, Serrato and Rosenzweig advise companies to conduct gap assessments at least annually to identify any business activities that are in non-compliance or pose a high risk to the company.

In a column last July for *Adweek*, Ben Plomion, CMO of computer vision and digital innovation firm GumGum, stated that "ongoing industry education is imperative to future survival." Proactive education, he explained, is necessary to minimize lawsuits and the negative impact to a company's reputation and credibility, and also provides a tremendous opportunity to establish greater public trust in the law.

To this end, the Interactive Advertising Bureau (IAB) created the "IAB Tech Lab GDPR Technical Working Group," whose mission is to share information on GDPR/ePrivacy and to engage technical leaders in contributing to solutions. By drawing on analysis from the IAB Europe GDPR Implementation Group and others in the global IAB network, the group works to develop and support technology and tools to facilitate legal compliance and self-regulation for the industry.

After more than a year of work with participants from across the digital advertising ecosystem, the IAB Europe Group issued a "Transparency & Consent Framework" that provides a standard infrastructure for passing information between publishers and their technology partners. The group encourages any company worldwide that needs to capture and use browser information of individuals located in the EU to make use of its framework. Without a framework, it says, publishers,

—continued on page 4

I guess those new Privacy Rules got the Boss thinking. He's even opted out of his "open door" policy.

SZABO ASSOCIATES INC.

PRESORTED
STANDARD
U.S. Postage
PAID
Atlanta, GA
Permit No. 747

Collective Wisdom® is a publication of
Media Collection Professionals,
3355 Lenox Rd. NE, Suite 945, Atlanta, Georgia 30326
Tel: 404/266-2464, Fax: 404/266-2165
Website: www.szabo.com
e-mail: info@szabo.com

GDPR —

—continued from page 3

advertisers, and advertising technology companies that work together to deliver digital advertising would have no common language to understand which consumers should see which advertisements. Publishers with business models already under pressure may lose access to an important source of revenue and revert to other approaches to fund content creation, such as putting content behind paywalls.

The IAB has listed a number of steps that every company in the digital advertising ecosystem should take to help them in their compliance journey. The checklist includes educating the team about the law; cataloguing personal data; reviewing policies; assigning responsibility for compliance; examining contracts; operationalizing rights; instituting compliance; and tackling transfers of data.

To help them comply with GDPR, many companies have chosen to contract with privacy technology vendors, an industry that has expanded rapidly over the last couple of years. In its 2018 Privacy Tech Vendor Report, the IAPP (International Association of Privacy Professionals) listed well over 100 firms in this burgeoning industry, organized by category according to their products and services. The report focuses on advice and tips from practitioners and consultants working for both large and small organizations across several industry verticals who have gone through the vetting, negotiating, implementation, and training phases of privacy technology acquisition. These privacy pros share some of their experience and insight to help other practitioners make smart decisions when determining if a vendor is needed and shopping for a privacy technology solution.

Into the Future.

GumGum's Plomion believes, as many do, that difficult change often results in unexpected opportunity. "As a lessening of our dependence on third-party data gradually moves closer to the forefront of the advertising ecosystem," he says, "we can likely expect to see a great deal of innovation and creativity in the coming months and years as GDPR compliance becomes embedded in the digital fabric of how we do business as marketers and solution providers."

In the meantime, media companies should take advantage of resources such as the IAB and IAPP to stay abreast of new developments and entrants into the privacy technology industry. These resources, as well as media industry trade associations, can provide a wealth of knowledge and experience for having stayed ahead of the pack with GDPR compliance. Additionally, because federal and state governments are pursuing privacy regulation at an increased pace, organizations must stay informed on pending and enacted legislation. ♦