US - NEW YORK

Della M. Hill

Associate, MacDonald Weiss PLLC

hill@macdw.com
irglobal.com/advisor/della-m-hill
+1 646 513 3280

An associate at MacDonald Weiss in New York City, Della M. Hill works on privacy, corporate, M&A, commercial, licensing, tax, and other business-related matters for US and international clients.

Della is certified by the International Association of Privacy Professionals (CIPP/US) and devotes a substantial amount of her time advising clients on the complex regulatory framework applicable to consumer-facing businesses. She provides guidance and support for compliance with US state and federal laws relating to data privacy, e-commerce contracts, marketing and promotional campaigns such as sweepstakes and contests, social media content, endorsements, and influencer campaigns, and other highly regulated consumer-based business activities.

macdw.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

New York is strongly focused on data privacy, but the law is still developing. The great challenge for affected businesses is dealing with the uncertainty about how the law will balance pro-consumer and pro-business interests—and what precisely it will require for compliance.

New York has passed a number of specific laws relating to data privacy and security, reflecting an increased commitment to the protection of consumer data. For example, the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act"), which strengthens and expands data protection and breach notification requirments, was signed into law this year.

However, a proposed comprehensive state privacy law (the "New York Privacy Act" or "NYPA"), referred to the New York State Senate Consumer Protection Committee for consideration, has faced strong resistance from business-oriented lobbyists. The NYPA has similarities with – and in some ways goes beyond – both the California Consumer Privacy Act ("CCPA") and the European General Data Protection Regulation. Although the proposed law failed to pass during the last legislative session, pro-consumer groups are strong and vocal in New York, and the NYPA may reappear in 2020.

Another challenge is that any New York-based company with an online presence is almost certainly reaching customers throughout the US and thus almost certainly is required to comply with multiple US privacy laws beyond those of New York. The patchwork nature of US privacy law, and especially the inconsistencies between the laws of the various states, makes compliance difficult. This challenge will become only more difficult to manage in the next decade, especially as technology continues to develop, unless Congress acts to pre-empt state law in this area or unless the states agree to follow common principles (as they have in some areas of commercial law).

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

New York has demonstrated an increased commitment to the enforcement of data privacy and security rules. In September 2019, the New York Attorney General filed suit against the parent company of Dunkin' Donuts for failing to safeguard the data of thousands of customers who were targeted in a series of cyberattacks, stating in a press release: "My office is committed to protecting consumer data and holding businesses accountable for implementing safe security practices."

The recently passed SHIELD Act increased civil penalties for violations of breach notification requirements and extended the statute of limitations on enforcement actions. Any business that collects personal data of New York residents will need to pay particular attention to compliance obligations under this new law, which applies to any business – regardless of size or location – that collects personal data of New York residents.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

One immediate impact of GDPR is that New York-based companies with a global customer base must decide whether to comply with the GDPR for all customer data collected (for example, obtaining explicit consent from both US and EU customers for the processing of certain types of data), or to maintain separate databases and offer differing degrees of protection to each. The latter may be difficult in practice, as it requires, for example, multiple versions of web pages on a global e-commerce website.

A more consequential impact of GDPR may be that New York consumers have become increasingly aware of the expansive (and potentially unchecked) collection, use, and disclosure of their personal data and, learning of the measures to protect the data of EU consumers under GDPR, may have developed expectations for similar protection in the US. The proposed NYPA is evidence of this impact.

Although it may be challenging for New York companies to build procedures that are simultaneously compliant with US law and the GDPR, it does provide an opportunity for international cooperation because this is the first time, generally speaking, that US companies without foreign branches or subsidiaries have had to pay attention to non-US law.

MacDonald Weiss offers a compelling combination of elite multinational law firm and Fortune 100 in-house experience, an accessible and nimble style, and value for money. In short, top tier sophistication on a human scale.

We serve mid-market companies, start-ups and emerging companies, family offices, angel, VC, and private equity investors, and large companies for whom a large firm is overkill for the task at hand. We focus on overseas clients with US activities, companies expanding into or out of the US, domestic early-stage companies, and investors.

MacDonald Weiss covers the core business-related practice areas: corporate, M&A, securities, finance, commercial, and tax. We also act as US – or global – outside general counsel.

| Data Privacy in New York

1. Pay attention to the overall data privacy framework

Pay close attention to the rapid developments in data privacy law – both in and outside of New York. A business collecting data from New York residents will likely need to comply with laws from multiple sources at the federal and state level (and, in some cases, with GDPR).

2. Know (and revisit) your client's data practices

Data flow mapping is a crucial step toward compliance. You must understand your client's practices for the collection, use, and disclosure of data (and any changes in these practices) to identify the data privacy laws that may apply at any given time.

3. Make sure your client follows through

Once your client's privacy practices are communicated to consumers, for example, in a website privacy policy, your client must actually follow the practices described. Failure to do so may not only lead to violations of the applicable privacy laws, but it may also violate the Federal Trade Commission Act, which requires that a company actually follow through on its promises and representations to consumers.

4. Do not forget service providers

Your client may be liable for data privacy violations by third parties engaged to collect, process, manage, or store customer data on your client's behalf. You should review any agreements between your client and such parties (e.g., cloud service providers) to ensure that they are contractually obligated to meet applicable data privacy obligations when acting on your client's behalf.