Protecting Data Privacy Starts with You

Technology, Privacy, and eCommerce

Emerging privacy laws present challenges for in-house counsel on a dual front: via client services and through their internal operations.

Lawyers, whether working in-house or for a firm, tend to operate from the mindset that legal work is protected and always confidential. That does not mean, however, that privacy laws do not apply to legal work. Nor does it mean that law firms or lawyers are invulnerable from attacks.

In the 2019 ABA Legal Technology Survey Report, 26 percent admitted their law firm experienced a breach. The factors that make a law firm an enticing target to thieves also make in-house legal departments similarly alluring: They are repositories of sensitive information, whether that means personal or business data.

The ABA Formal Opinion 477R states that "[A] lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

The opinion lists seven steps lawyers should consider when protecting information:

1. Understand the nature of the threat.
2. Understand how client confidential information is transmitted and where it is stored.
3. Understand and use reasonable electronic security measures.
4. Determine how electronic communications about clients' matters should be protected.
5. Label client confidential information.
6. Train lawyers and nonlawyer assistants in technology and information security.
7. Conduct due diligence on vendors providing communication technology.

Although some believe the ABA opinion is meant for firm lawyers rather than in-house counsel, the considerations are essentially the same. In-house counsel certainly need to take steps to protect the information they handle because the data is inevitably sensitive. This means in-house counsel need to take steps to protect their devices as well.

Some of the actions in-house counsel should take are simple. Anytime your computer is not within your line of sight, make sure it is locked. This goes for other devices too. Your phone should be locked in general. Make sure to use a virtual private network and screen guards when working in front of other people, especially in public places, like during commutes on public transportation.

One of the most controversial protective measures centers on data deletion. Lawyers tend to prefer to hold on to all data, even when it's beyond its useful life. Laws are starting to require that personal data be destroyed when it is no longer needed for the purpose for which it was collected.

There are exceptions for data that are needed for legal defenses, compliance, and other related reasons, of which counsel should be involved. But lawyers are often one of the most common rulebreakers. They often export emails that should be deleted to a personal storage table, whether that means a personal email account or another unauthorized destination. Counsel should carefully consider why they are doing this and the justification for violating policy.

However, there is another concern which counsel can specifically address: data retention timeframes for the company in general, especially email. Many IT departments cite legal holds as the reason not to permanently delete email, but if legal holds are not in effect, there is no reason to not delete

emails. Often, IT departments misconstrue the potential of a legal hold request with an actual legal hold request. There is generally more danger in retaining emails in perpetuity than the possibility of deleting the one rare email that holds the magic wand. In the compliance world, policies are in place for a valid reason and violating your own policies is almost worse than not having a policy in place.

Lawyers need to maintain an awareness of their roles in protecting data and the sensitivity of the data they manage. There are some basic steps to take to put in privacy and security practices that are simple yet effective. Be a model for data privacy at your company by following procedures and deleting data.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.