



## **Privacy Now: Predicting 2021's Legal Tech Trends**

**Technology, Privacy, and eCommerce**



This past year saw a lot of movement in areas of law and technology. Some were not on the prediction radar at all, and some had long been identified but undervalued. Before making predictions for 2021, I looked back at my predictions for 2020:

1. Privacy program management and security tools
2. Vendor management tech, including contract management with artificial intelligence (AI)
3. Virtual law practice
4. Alternative legal solutions
5. Life integration tools

Even given the unexpected events of 2020, the predictions were still relevant — perhaps eerily so. However, 2020's surprises will not pass quickly or easily. And that impacts the predictions for 2021. After much consideration and research, my predictions for the hottest legal trends in 2021 are below, recognizing that there is carryover from last year's list and their critical status has only increased. Here are the top five predictions for 2021:

1. Data protection and information governance, with a focus on security
2. Full lifecycle vendor management for insight and oversight, including the use of AI
3. Virtual offices / remote work integration
4. Internet of Everything for legal ops
5. Alternative legal services and service models

---

## 1. Data protection and information governance, with a focus on security

With the exponential growth of global privacy and data protection laws, such as Brazil's *Lei Geral de Proteção de Dados Pessoais* (LGPD) and the California Privacy Rights Act of 2020 (CPRA, the successful ballot initiative that will amend the current California Consumer Privacy Act of 2018), companies that have not been focusing on privacy law will need to do so quickly. As anticipated, laws such as the LGPD and Canada's proposed Digital Charter Implementation Act are based heavily on the EU's General Data Protection Regulation (GDPR). The trends in privacy and data protection laws span three major areas: individual rights, security, and enforcement.

Another trend in privacy and data protection for businesses is the involvement of the legal department. The counsel's office has typically been involved at some level, but with the complexity, scope, and penetration of privacy law and processes, legal has been increasingly engaged. The engagement stems from privacy-by-design aspects in product and service development, contracts with clients and vendors, following rules for advertising (more on this one below), and notices about the company's practices with individual data.

The security aspect is also becoming more ingrained with privacy programs — either in collaboration or by rolling the privacy program into the realm of the chief information officer, the CIO. Unlike prior legislation, security is now becoming a major element of the legal requirements. For example, the CPRA requires an annual security audit. The New York State Cybersecurity law, from the Department of Financial Services, requires strict cybersecurity requirements on all financial institutions and financial services companies.

With the new regulations comes the need for tools to manage the process. Each year, the number of third parties offering tech solutions for privacy and data protection is increasing. In 2017, there were 44 vendors listed in the International Association of Privacy Professionals tech report. "Since that time, the growth in new vendors has followed a hockey-stick trajectory," the [latest report](#) notes, which includes 343 privacy tech vendors. Last, privacy program management includes employee training and confidentiality management during and upon termination. The legal department should be involved in this training to the extent that it determines the timing and type of training, ensures the training meets compliance requirements, and has training specialized to legal actions provided for the legal department.

## 2. Full lifecycle vendor management for insight and oversight, including the use of AI

The ubiquitous need to control risk by vetting vendors remains a growing area of both concern and focus for emerging tech. The problem remains and a successful solution remains to be found (although I hear whispers of a start-up that is moving in the right direction). The problem is that the new concern and legal requirements around transfer of personal information to third parties are layered on top of traditional vendor outsourcing concerns and needs for due diligence and risk balancing. Unfortunately, the traditional solutions fall short.

The traditional solutions, stemming from contract management and financial risk, and perhaps regulatory quality control, are not successfully managing personal information under data protection laws. Further, the specialization of the cloud providers (whether software, platform, or infrastructure) is successfully driving cloud mobility at the same time that data is being created at an astronomical

---

rate.

According to [TechJury](#):

- 1.7MB of data is created every second by every person during 2020.
- In the last two years alone, 90 percent of the world's data has been created.
- 2.5 quintillion bytes of data are produced by humans every day.
- 463 exabytes of data will be generated each day by humans as of 2025.

That's a lot of data. And when you outsource the management of this data, whether personal or business, you need to feel secure (literally) in how the vendor is managing your property. But given the amount of data, increasing complexity of operations, and the trend towards decentralized management (especially in the prevalence of remote work), gaining insight is just as critical as oversight.

Companies must have visibility across the vendor environment in order to manage consistency in contracts, identify outliers, and gain efficiencies in utilization of third parties. Although a strong contract management system is typically the first step towards management of vendors, it is not the magical tool to address all needs for vendors and other third parties. There are needs in identifying the right vendors, comparing vendors, along with onboarding them, paying for the products or services, annual review, and managing the offboarding. This is where AI, or machine learning, will make the largest impact. Contract management is ready for its transformation, from inception to analysis to crisis management.

This legal trend is directly related to inside counsel given the connection to contracts, data protection agreements, risk control, protecting corporate assets, and M&A activities. It is not surprising that this one remains one of the hottest trends in legal tech, because of the need, the universe of offerings, and the available solutions.

### **3. Virtual offices and remote work**

This one is not a surprise! Many in-house counsel have realized for years that working remotely is a viable alternative, but the tradition of being present and visible has long pervaded the legal work expectations. Yes, the current environment has dictated relaxing those edicts and companies are now realizing that even attorneys can work remotely.

But working remotely is not without its risks, especially for attorneys — both inside and outside counsel. Technology must be utilized effectively and consistently. Further, companies must ensure that technology is used with permission and that employees do not resort to whatever is convenient and readily available. This is where a lot of attorneys can go wrong; finding a technology that is easy to use and accomplishes the task even if the tech has not been vetted according to the vendor management processes described above.

Often freeware, which does not trigger contract reviews or even accounts payable, is one of the largest vulnerabilities for data leakage. Some great examples include free file sharing, e-faxing, and dictation tools. But with virtual offices, you need to also consider that all-in-one devices (copy, scan, fax) typically have hard drives, which may be capturing confidential information. Voice-activated smartphones also record without the user being aware of the recording. And devices may be configured to sync with native apps.

---

Often freeware, which does not trigger contract reviews or even accounts payable, is one of the largest vulnerabilities for data leakage.

Plus, the younger generations tend to implement “shadow IT” because they are accustomed to working with tech and have their preferences. This creates a risk to operations without having centralized visibility or control.

Last, we have all heard stories of video calls with the glut of embarrassing activities and the prevalence of pets and kids. Virtual offices have become a case of living at work rather than working from home. One of the biggest tech advances in virtual offices needs to be the ability to turn the tech off.

## 4. Internet of Everything for legal ops

Highly related to the above prediction, another move that has been occurring but is gaining momentum is the connectivity and integration of applications. The Internet of Things (IoT) is becoming the [Internet of Bodies](#) regarding personal tracking, and the Internet of Everything is not an inaccurate way to conceptualize this movement.

Tech start-up companies seem to leverage APIs (application programming interfaces) as part of their go-to-market strategy to maximize their impact. This occurs in legal tech as much as other markets, but now the younger generation of attorneys are making this a reality for expected work processes. These connected processes, technology, applications, and accessible work tools are prevalent and increasing in sophistication, usability, and mobility.

Applications in this growth area range from general business to legal specialization software. A primary example of a general business use is document sharing and workflow across devices, where multiple people can edit the same document simultaneously and transition between computers and cell phones. Other examples include document scanning with camera phones, project management, and business card readers. Many of these general business use cases have levels and configurations that cater to the needs of attorneys with confidentiality provisions, which also assist in maintaining privilege.

The legal-specific use cases tend to cater to law firms with time tracking, but have expanded to include managing outside spend with visibility into time tracking and case management that is easily configurable for in-house counsel to collaborate with outside counsel. There are companies that now specialize in legal operations, like [BigFork Tech](#), and are designed to function around how legal offices work in-house. Legal ops is how corporate legal departments operationalize their activities, by applying business and technical processes to the practice of delivering services to their internal clients. Other examples of legal use cases include law dictionaries, legal research, listserv collation, and document templates.

The examples above address the automation, but once you add in the integration, the IoT portion, one can visualize how integrated apps can facilitate the workload for attorneys. On top of that, add in the personal apps for posture, exercise, nutrition, and general well-being — and suddenly you reach the next phase, what I term the Internet of Everything (IoE). This next level will use eye motion and body sensors to identify and automate common tasks. Imagine looking at an email attachment, blinking once to select it, turning to look at the electronic folder options, and blinking twice to move it. Repetitive motion syndrome may become a malady of the past.

---

Even if we point instead of blink — like Tom Cruise in *Minority Report* or Robert Downey Jr. in *Iron Man* — that would be a huge leap in legal tech and enable us to almost work at the speed of thought.



Legal technology isn't far behind.

Frankly, yes, the loE may be a bit further off than 2021, but 2021 will get us closer with integration, automation, and mobility. This prediction is for the start of the tech in this direction, not the full realization and common adoption.

## **5. Alternative legal services and service models**

This prediction, like many of the ones above, carries over from the 2020 predictions. COVID-19 interfered with the natural lifecycle of tech innovation and adoption because companies were forced to rapidly deploy remote workforces. Many companies did not survive the trauma and others were forced to scale down tremendously. Thus, the full adoption of alternative legal services, non-lawyer firms providing law-related services that not require law degrees, was not realized. However, the scaleback may very well propel the alternative legal service model forward this year. These services comprise document review, legal research, and IP management such as maintaining filing dates and renewals.

As we start moving towards the loE above, alternative legal service providers will become more common either as standalone firms or alternative models offered through traditional law firms, which realized in 2020 that being in the office is not a requirement to deliver quality legal services. Why pay a lawyer US\$400 an hour when a paralegal can provide the same services for US\$50 an hour for low-risk, high-volume, repetitive tasks?

---

In fact, [Arizona made history this year](#) by permitting non-lawyers to own interest in law firms under alternative business structure models and to practice in limited areas of law, such as administrative law and debt collection. Legal Paraprofessionals (LPs) will have to be “admitted” to the Arizona bar and follow the same ethical rules. A few other states have implemented similar rules or experiments, such as Utah and Washington.

In-house counsel need to evaluate use of these services and determine how best to structure their outsourced legal needs. Expect outside counsel to propose alternative pricing models to counter this movement as they may start devoting a piece of their traditional practices to a leaner paradigm. Either structure of which offers savings and efficiency to outsourcing.

Here’s to hoping 2021 brings pleasant developments!

[K Royal](#)



Global Chief Privacy Officer

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](https://twitter.com/heartofprivacy) on Twitter, or [www.linkedin.com/in/kroyal/](https://www.linkedin.com/in/kroyal/).