In this landmark year for data privacy, are US and UK executives as prepared as they think?

July 2023
# Table of Contents

**Executive Summary** ............................................................ 3

**Key Findings** ................................................................. 3

**A Changing Global Data Privacy Law Landscape** ............................................. 8
  • Preparedness ................................................................. 11
  • Progress ................................................................. 12
  • Challenges ................................................................. 14
  • Concerns ................................................................. 15

**Emerging Technologies: AI, Biometrics and Geolocation** ............................................. 18
  • AI on the Rise ................................................................. 19
  • The Expanding Use of Biometric Data ................................................................. 23
  • Geolocation Data Raises Concern ................................................................. 26

**Conclusion: Preparing for the Year Ahead** .................................................. 28
  • Methodology and Demographics ................................................................. 30

Privacy and Cybersecurity Team .......................................................... 34

Womble Bond Dickinson at a Glance .................................................. 36
Executive Summary

2023 is shaping up to be a landmark year for data privacy, on both sides of the Atlantic. In the US, four new state laws go into effect – two on July 1 – while California is expanding its already robust requirements, and several other states have enacted or proposed privacy legislation of their own. Across the pond, the EU-US Data Privacy Framework nears implementation as negotiations around other global agreements – such as those between the European Union and a post-Brexit United Kingdom – intensify.

Against this backdrop, Womble Bond Dickinson’s second annual survey report analyzes the fast-evolving global data privacy law landscape and, for the first time, includes over 200 respondents from both the US and UK.

The survey finds that as data privacy compliance gets progressively more complex, only about half of executives are “very prepared” to meet these standards. What’s more, given our global respondents’ lack of readiness with regard to such early measures as understanding where all their data sits across their organization, even these executives may not be as prepared as they think.

Drawing on insights from business leaders who play a leading or supporting role in data privacy issues – nearly half of whom are in the C-suite – our report illuminates how organizations across industries are preparing for regulatory challenges, the growing use of biometric data and artificial intelligence (AI), differences between operating in the US, the UK, Europe and more.

Key Findings

- ~50% of US and UK organizations say they are “very prepared” to address data privacy laws in both the US and Europe.
- 34% of all respondents have conducted data mapping and understand data practices at their organization.
- 55% of US respondents are concerned with enforcement actions around geolocation data privacy laws, while 50% say as much about litigation – a significantly higher share than their UK counterparts, at 45% and 36%, respectively.
When it comes to data privacy laws, are organizations as ready as they think they are?

The survey also uncovered that many respondents in the UK and US who say they are very prepared may not have taken the measures needed to justify such a claim. For instance, while many companies might implement external-facing actions, such as putting a cookie banner on their website or updating privacy policies, just 34% of all respondents say they have conducted data mapping and understand data practices across the organization.

“Companies are often under-resourced and have to focus on cosmetic changes by updating public-facing content; however, this doesn’t eliminate the inevitable need to build out back-end requirements to truly operationalize the compliance requirements,” says Tara Cho, partner and chair of the Privacy and Cybersecurity Team for Womble Bond Dickinson (US).

“This potential lack of readiness is evident in other areas as well. For instance, 50% of respondents doing business in the EU and/or UK say understanding the data held within their organization is a key hurdle, while 45% cite increasing their budget. Meanwhile, nearly 60% of executives with operations in the US view tracking the status of legislation and the differences between state laws as a challenge – yet only 42% have completed comparisons of state privacy law frameworks. And as several state data privacy laws near or reach effective dates, executives with...
operations in the US are feeling less confident in their preparedness than in 2022: Only 45% say they are very prepared, compared with 59% in last year’s survey.

**UK respondents more prepared than US counterparts**

Given the more established General Data Protection Regulation (GDPR) in the UK and EU, as well as the Data Protection Act 2018 (DPA) in the UK, it tracks that more respondents with operations on the continent feel very prepared to meet these requirements – particularly our UK-based respondents (59% of whom say they are very prepared for the GDPR and/or DPA, compared to only 44% of those with US headquarters).

UK respondents are also more comfortable with the impact of privacy regulations on their ability to conduct cross-border business. Forty percent of UK respondents (versus 35% in the US) say these regulations add extra costs but are manageable, while only 10% (versus 17% in the US) believe regulations are a major impediment to such business.

“Overall, these findings tell us that, while cross-border data transfers remain a challenge, many businesses are managing and even seeing value in associated regulations,” says Andrew Parsons, a UK-based partner at Womble Bond Dickinson.
Parsons – who focuses on commercial disputes around information rights, privacy and other technology-related issues – adds that: “Though much remains in flux, if and when these rules stabilize, they can have a positive long-term impact.”

**Growing adoption of biometrics, geolocation and AI brings new opportunities – and concerns**

The majority of UK and US respondents are already using fingerprints, facial recognition and other biometric data. However, new technologies come with new compliance challenges and litigation risks.

Fifty-nine percent of UK respondents indicate that their organizations currently leverage biometric data – and 64% of US respondents say the same, a five percentage point jump for that group from 2022. While most are using fingerprints to generate such data, largely for initial identification or authentication purposes, not insignificant numbers in the US and UK are drawing biometric information from iris recognition (28%), finger/hand veins (24%), heartbeat (8%) and even brain waves (5%). Data privacy litigation will increasingly play a role here, particularly as more and more states and municipalities enact biometric-related regulations.

The use of geolocation data creates similar issues. Forty percent of US respondents (and 32% of those in the UK) say they are very concerned about privacy laws that include specific restrictions on collecting and using such data for targeted marketing purposes. Litigation and enforcement actions – especially among US respondents – were named as top concerns.

As advances in AI generate global headlines, our survey tracks the technology’s accelerating adoption across the business world – for more traditional applications such as data analytics, as well as content generation and other newer uses. More than 1 in 5 respondents (22%), for instance, have started using AI in the past year alone, and only 19% aren’t using it at all. Ethical and legal risks were cited as key obstacles by a significant number of respondents (45% and 34%, respectively).

“Whether it’s evaluating loan applications, filtering qualified candidates for a new job posting, or any number of other use cases, AI tools make complex decisions all the time,” says Ted Claypoole, partner at Womble Bond Dickinson and head of the firm’s US IP Transactions Team. “That’s what they’re there for. The question is, are they doing it in a way that’s improper from a societal and legal standpoint?”

As these trends accelerate in 2023 and beyond, so too will the complexity of the data privacy law landscape. Our hope is that this year’s report provides benchmarks, insights and guidance to help organizations in their compliance journeys.
Authors

Tara Cho
Partner
Chair, Privacy and Cybersecurity Team (US)
tara.cho@wbd-us.com

Ted Claypoole
Partner
Privacy and Cybersecurity Team (US)
Lead, IP Transactions Team
ted.claypoole@wbd-us.com

Andrew Kimble
Partner
Privacy and Cybersecurity Team (UK)
andrew.kimble@wbd-uk.com

Andrew Parsons
Partner
Privacy and Cybersecurity Team (UK)
andrew.parsons@wbd-uk.com

In the charts and analysis, responses to some questions do not add up to 100% due to rounding, and some exceed 100% because respondents were invited to select more than one answer. For the full survey methodology and a breakdown of respondent demographics, see pages 30-33.
A Changing Global Data Privacy Law Landscape
A Changing Global Data Privacy Law Landscape

Organizations are confronting new data privacy laws in several US states, as well as stepped-up oversight of GDPR investigations in the EU and uncertainty over the regulation of transatlantic data flows. Meanwhile, in the UK, new proposals that aim to relieve businesses of some of the GDPR’s more strict requirements could jeopardize current legal agreements between the UK and EU.

This year, privacy laws have or will become effective in Virginia (January 1), Colorado and Connecticut (July 1) and Utah (December 31). On the West Coast, the California Privacy Rights Act (CPRA) officially amends the CCPA, though a judge recently declared these new rules wouldn’t be enforceable until next March.

While these laws differ – Utah’s legislation is more business-friendly than Colorado’s and Connecticut’s, for example, and California’s is the only one that enables a private right of action – Cho says the common thread is “giving consumers power as to how they are tracked online.”

With that said, the newly amended CCPA is in a league of its own, raising the bar for compliance.

“All of these five new state laws use the word ‘Consumer,’ and I think we all initially thought it meant an individual customer,” Matthew A. Cordell, Vice President & General Counsel for Privacy and Technology, VF Corporation, said on a recent Womble Bond Dickinson panel. “But on January 1 [2023], the law in California began to apply to employees, job applicants, former employees, beneficiaries of company benefits policies and independent contractors, as well as B2B contacts, all for the first time. That’s a formidable scope to expand privacy rights to.”
This development creates a host of challenges. For instance, should companies with multiple locations treat California employees differently? If they do, will employee morale take a hit? Understanding when and how to apply various CCPA exemptions is crucial, too, as is the necessity of knowing where employee records are housed.

**ACTION:** Understand when and how to apply various CCPA exemptions – and where employee records are housed.

With states including Indiana, Iowa, Montana, Tennessee and Texas passing legislation of their own this year – largely modeled after Virginia’s model – we can see a common thread of core principles running through these state laws. That may be welcome news for the 88% of respondents in the 2022 iteration of this survey who wanted to see a federal data privacy law replace the patchwork of state laws. That said, distinctions will continue to appear in these laws as political divides persist.
Preparedness

In this increasingly complex environment, it’s no wonder that only 53% of those doing business in the EU and/or UK say they are very prepared for the GDPR and/or DPA, despite those requirements having taken effect several years ago. What’s more, fewer than half of respondents with operations in the US (45%) say they are very prepared to address state privacy laws. On the bright side, those headquartered in the UK are particularly prepared for EU regulations (59% versus 44% of US-headquartered respondents), while those based in America are more prepared for US regulations than their UK counterparts (49% versus 40%).

At the industry level, the combined share of retail and financial services industry respondents from the UK and US who feel “very prepared” regarding US state privacy laws dropped to levels below 40%, and to less than 50% when it came to the GDPR and/or DPA.

“Europe has long been ahead of the US when it comes to data privacy laws – they’ve had one in effect since 1995, and the GDPR was adopted in 2016 – so it makes sense that UK respondents are well positioned to comply with these regulations,” says Andrew Kimble, a UK-based partner at Womble Bond Dickinson.

Kimble, who focuses on data protection and privacy, adds that: “Employees at all levels of the organization in the UK tend to be aware of the GDPR and DPA given all the steps companies need to take.”

Please indicate your organization’s level of preparedness when it comes to the following data privacy laws and regulations:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>US Consumer Data Privacy Legislation (State Privacy Laws)</td>
<td>40%</td>
<td>49%</td>
<td>45%</td>
<td>36%</td>
<td>13%</td>
<td>6%</td>
</tr>
<tr>
<td>[Asked to those doing business in the US]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GDPR and/or DPA Act 2018 (DPA 2018)</td>
<td>59%</td>
<td>44%</td>
<td>53%</td>
<td>35%</td>
<td>10%</td>
<td>2%</td>
</tr>
<tr>
<td>[Asked to those doing business in the EU and/or UK]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022 (US only)</td>
<td>5%</td>
<td>5%</td>
<td>31%</td>
<td>35%</td>
<td>10%</td>
<td>6%</td>
</tr>
</tbody>
</table>
Yet our survey illuminates that even those who believe they are very prepared may not be as ready as they think.

While 70% say they have designated an internal project manager or owner and 58% say they conduct regular training of staff on data privacy and compliance, less than half of the overall respondent pool have taken the following steps: engaged outside legal counsel (42%), participated in a peer group to keep abreast of changes (40%) or developed a task force/oversight counsel to track privacy law changes (35%).

Most importantly, only 34% say they have conducted data mapping and understand data practices across the organization. In other words, many say they are prepared to comply with data privacy laws without having a full picture of what data they actually hold.

For respondents with operations in the US, only about 4 in 10 have implemented the following measures to comply with state data privacy laws: conducted comparisons of state privacy law frameworks (42%, up from 35% last year), updated privacy policies (41%), developed systems to process and respond to data privacy rights requests (41%), set metrics and specific goals (39%), and drafted/updated agreements with third parties (39%). Only 36% have planned and conducted data assessments, down from 43% of US-only respondents surveyed last year – though that could be a result of the California Consumer Privacy Act not having yet described what assessments need to be done.

### What is your organization’s status on each of the following data privacy measures?

<table>
<thead>
<tr>
<th>Measure</th>
<th>Completed</th>
<th>In Progress</th>
<th>Considering or Planning</th>
<th>Not Planning at This Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designate an internal project manager or owner</td>
<td>70%</td>
<td>18%</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Conduct regular training of all staff on data privacy and compliance</td>
<td>58%</td>
<td>24%</td>
<td>11%</td>
<td>15%</td>
</tr>
<tr>
<td>Engage outside legal counsel to advise on legislative changes</td>
<td>42%</td>
<td>24%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>Participate in a peer group within industry to keep abreast of changes</td>
<td>40%</td>
<td>24%</td>
<td>12%</td>
<td>14%</td>
</tr>
<tr>
<td>Develop a task force or oversight counsel to track domestic and/or cross-border changes</td>
<td>34%</td>
<td>20%</td>
<td>17%</td>
<td>20%</td>
</tr>
<tr>
<td>Conduct data mapping and understand data practices across the organization</td>
<td>32%</td>
<td>20%</td>
<td>17%</td>
<td>20%</td>
</tr>
</tbody>
</table>
“Senior-level employees may be overly optimistic when it comes to compliance preparedness because they’re not in the weeds – and so don’t even know how many weeds there are,” says Claypoole.

“This is understandable, of course, especially in the US, where this is all relatively new,” Claypoole notes. “Data privacy is an engineering, technology and risk management issue, and it’s rare to have one person who understands all three. That’s why organizations should view this as a team effort.”

To this end, Claypoole recommends creating a list of the workstreams involved in implementing a solution and which employees need to be involved. This may include working with service providers, contractors and vendors, as well as employees.

**Please indicate your organization’s progress in terms of the following actions to comply with state data privacy laws in the US:**

<table>
<thead>
<tr>
<th>Action</th>
<th>2022 US only</th>
<th>2022 US only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct Comparison of State Privacy Law Frameworks</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Update Privacy Policies</td>
<td>41%</td>
<td></td>
</tr>
<tr>
<td>Develop Platforms and Systems to Process and Respond to Data Privacy Rights Requests</td>
<td>41%</td>
<td></td>
</tr>
<tr>
<td>Set Metrics and Specific Goals / Deadlines to Track Progress</td>
<td>38%</td>
<td></td>
</tr>
<tr>
<td>Draft or Update Agreements with Third Parties</td>
<td>37%</td>
<td></td>
</tr>
<tr>
<td>Plan and Conduct Data Assessments</td>
<td>43%</td>
<td></td>
</tr>
</tbody>
</table>

**ACTION:** Create a list of the workstreams involved in implementing a data privacy solution that includes which employees, service providers, contractors and vendors need to take part.
Challenges

Keeping abreast of the latest changes represents the biggest challenge for respondents on both sides of the Atlantic. Hurdles include tracking the status of legislation and differences between state laws in the US (59%), as well as adapting to new/changing requirements in Europe (55%).

The team effort required to address data privacy issues also leads to numerous operational issues – especially in the US. For those doing business in the states, key challenges include budget increases (52%), lack of available staff (42%), obtaining management approval and support to prioritize changes (30%), and the lack of an appointed leader (21%).

By contrast, each of these selections was chosen by fewer respondents doing business in the UK and/or EU – fitting, given their longer experience with the GDPR and/or DPA, as well as the GDPR mandate to have a data privacy officer. For that group, 45% say budget increases are a challenge, while 39% cite lack
of available staff, 23% cite obtaining management approval and support, and just 10% cite the lack of an appointed leader. Understanding the data held within the organization is also a key challenge for both groups – which tracks with organizations’ lack of progress on data mapping.

**Concerns**

In an increasingly global – and digital – business landscape, the ability to transfer data across borders is paramount.

When it comes to transferring data from Europe to the US, however, regulatory mechanisms for doing so are in flux following the Court of Justice of the European Union’s 2020 invalidation of the EU-US Privacy Shield framework. Though the Biden administration has proposed a successor framework to address these concerns – the Trans-Atlantic Data Privacy Framework – it is unclear as of yet whether it will pass the GDPR’s adequacy standard. The US and UK, meanwhile, are currently working through their own agreement aimed at creating a “data bridge” for data flows between the two nations.

Despite these uncertainties, our survey gives some indication that data privacy regulations are generally good for cross-border business – especially for UK respondents, who are more experienced with existing standards. Roughly a third of all respondents say that regulations add extra costs but are manageable and that
they encourage international business by providing assurance that data will be treated properly in other countries. Only 10% of UK respondents – and 17% in the US – say data privacy regulations are a major impediment to cross-border business.

When it comes to big-picture concerns around data privacy, respondents ranked data breaches and cybersecurity as the number one issue – with UK executives expressing particular concern. Retail and financial services respondents indexed higher than all other industries in terms of data privacy concerns, with 42% and 41%, respectively, selecting “high level of concern.”

US respondents’ second-ranked issue is litigation and regulatory enforcement action – which plays out in later sections of this report – while in the UK the runner-up spot is split between loss of customer loyalty/trust and cost of compliance with privacy laws. Interestingly, US respondents are more concerned about not fully utilizing data to maximize sales/revenue and less concerned with the cost of compliance than their UK counterparts.

Cho speculates that this result speaks to differences in how data privacy laws are shaped in the EU and UK versus the US.

“Privacy is a fundamental right in the EU, and the GDPR and its predecessor Directive have provided longstanding legal frameworks to protect those rights. In contrast, US laws have historically been sectoral and reactionary – for instance, what happens if personal data is breached. These new state omnibus privacy laws impose proactive requirements and the main impetus is to empower consumers with rights over their data, particularly when that data is being monetized.”

— Tara Cho, Partner, Womble Bond Dickinson (US)
What is your organization’s level of concern when it comes to each of the following data privacy issues? Please rate each one from 1 to 5, where 1 = low level of concern and 5 = high level of concern.

**MEAN & RANK**

<table>
<thead>
<tr>
<th>Issue</th>
<th>US</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA BREACHES / CYBERSECURITY</td>
<td>3.60 (1)</td>
<td>3.99 (1)</td>
</tr>
<tr>
<td>LITIGATION / REGULATORY ENFORCEMENT ACTION</td>
<td>3.57 (2)</td>
<td>3.52 (4)</td>
</tr>
<tr>
<td>LOSS OF CUSTOMER LOYALTY / TRUST (IF PERCEIVED TO NOT BE RESPECTING THEIR PRIVACY)</td>
<td>3.43 (4)</td>
<td>3.62 (2)</td>
</tr>
<tr>
<td>NOT FULLY UTILIZING OUR DATA TO MAXIMIZE SALES / REVENUE</td>
<td>3.50 (3)</td>
<td>3.38 (5)</td>
</tr>
<tr>
<td>COST OF COMPLIANCE WITH PRIVACY LAWS</td>
<td>3.40 (5)</td>
<td>3.62 (2)</td>
</tr>
</tbody>
</table>

**Global Data Privacy Law Survey Report  July 2023**
Emerging Technologies: AI, Biometrics and Geolocation
Emerging Technologies: AI, Biometrics and Geolocation

AI on the rise

As the use of ChatGPT and other generative AI applications goes mainstream, our survey reveals that businesses are accelerating their adoption of the technology: 22% of all survey respondents say they have started using AI in the past 12 months alone — and only 19% are not using it at all. However, nearly half of technology industry respondents report usage of the technology for five years or longer, reflecting that it was already baked into many business operations before the recent advances in generative AI.

How long has your organization been using artificial intelligence (AI) in various aspects of its business?

- Longer than five years: 14%
- One to five years: 45%
- Past 12 months: 22%
- Not using AI: 19%

INDUSTRIES
- Construction
- Professional / Business Services
- Government
- Financial Services / Banking
- Education
- Retail

Organizations we surveyed have the budget available to support their use of AI. The majority are either already making material investments in such technology (25%) or plan to within 12 months (26%; only 7% say it is not part of their plans. Those headquartered in the US showed very little deviation from UK-based organizations.

When do you expect your organization to make material investments in AI technology?

- We are already making material investments: 25%
- Within 12 months: 26%
- Within 1 to 2 years: 18%
- Within 3 to 5 years: 14%
- Within 6 to 10 years: 3%
- AI investment is not part of our plans: 7%
- Unsure at this time: 6%
The applications reported for AI are wide-ranging. Half of respondents or more are already using it (or planning to use it in the next year) in nearly all the ways we asked about, from data analytics and automation of business processes to supply chain optimization, search engine optimization, customer service assistance, product recommendations and more. Notably, 36% are already using AI to generate content (via ChatGPT and similar applications), and another 24% plan to in the next year.

As expected, the growing popularity of AI comes with its own set of obstacles, led by ethical concerns and followed by a lack of understanding about the technology, unreliable results and legal risks.

“As AI comes into the fore, there are a number of moral concerns that might bleed into legal issues, such as AI’s proclivity to mirror societies’ own biases, therefore perpetuating historical social inequities,” says Parsons.

“There are also issues that could arise from these tools’ collection and processing of data, as well as intellectual property risks.”
Which of the following are key obstacles for your organization with regard to the use of AI? (Select all that apply)

- **COST**
- I DON'T HAVE ANY CONCERNS
- CUSTOMER CONCERNS / REPUTATIONAL IMPACT
- LACK OF QUALIFIED PERSONNEL TO IMPLEMENT CHANGES TO USE AI
- LEGAL RISKS
- UNRELIABLE / UNPREDICTABLE RESULTS
- LACK OF UNDERSTANDING ABOUT THE TECHNOLOGY / HOW IT MIGHT BENEFIT THE ORGANIZATION
- ETHICAL CONCERNS
- I DON'T HAVE ANY CONCERNS

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>US (%)</th>
<th>UK (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethical Concerns</td>
<td>48</td>
<td>43</td>
</tr>
<tr>
<td>Lack of understanding about the technology</td>
<td>41</td>
<td>35</td>
</tr>
<tr>
<td>Unreliable / unpredictable results</td>
<td>40</td>
<td>34</td>
</tr>
<tr>
<td>Legal Risks</td>
<td>34</td>
<td>35</td>
</tr>
<tr>
<td>Cost</td>
<td>34</td>
<td>31</td>
</tr>
<tr>
<td>Lack of qualified personnel to implement</td>
<td>33</td>
<td>33</td>
</tr>
<tr>
<td>Customer concerns / reputational impact</td>
<td>29</td>
<td>33</td>
</tr>
<tr>
<td>I don't have any concerns</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>
AI regulations are incoming around the world. The EU’s AI Act, which is expected to pass and could apply to businesses as soon as 2025, aims to be a global standard. In addition to segmenting applications of AI into four levels of risk, the law articulates specific requirements for ChatGPT and other providers of “foundation models.” Existing regulations, such as the GDPR and the EU’s Digital Services Act, could also be adapted to incorporate provisions around AI.

In the UK, the government has released a “pro-innovation” proposal for AI regulation, while the US is taking a patchwork approach, with federal actions aimed at advancing the White House’s AI Bill of Rights. Regulators such as the Federal Trade Commission (FTC) and the Equal Employment Opportunity Commission have released guidance, and numerous states and municipalities have put forth their own regulations. New York City, for instance, has imposed new requirements regarding automated decision-making tools, which various states appear to be taking up.

The UK will also host the first global summit on “AI Safety,” which will further shape the approach to regulating AI globally. While the date for the summit is yet to be confirmed, it will have a focus on harnessing AI “for good” and ensuring that AI is “developed and used in a way that is safe and secure.”

**ACTION:** With a complex patchwork of AI regulations on the horizon, intersecting with ethical considerations, it’s important to track the development of various laws and how (and where) they may impact your organization. Establishing governance frameworks and controls for the use of AI tools will also be paramount.
The expanding use of biometric data

The use of biometric data has grown in the last year – 64% of US respondents are currently using it, compared with 59% last year, and only 14% are not using it or planning to down the line – but so too have associated compliance risks. The UK shows similar levels of adoption, with 59% using it now, though a higher share of those respondents (20%) isn’t using the technology or planning to.

Several US lawsuits in the wake of Illinois’ 2008 Biometric Information Privacy Act (BIPA) have put biometrics in the spotlight – and lowered the bar for others to file successful BIPA suits. For instance, last October saw the first-ever jury verdict in a BIPA class action suit in *Rogers v. BNSF Railway Company*, wherein a group of truck drivers successfully sued the freight-rail operator over of its fingerprint scan security requirement at Illinois rail yards. The plaintiffs’ success could encourage other individuals to pursue their own claims.

Texas and Washington have their own biometric privacy laws, though neither provides a private right of action like BIPA, while the new state consumer privacy laws in California, Colorado, Connecticut, Utah and Virginia regulate the processing of biometric data. Other states and cities are likely to follow suit.

It follows, then, that for those respondents who are not considering using biometric data, data privacy compliance is a growing concern (17% said as much this year, versus 10% for the US only in 2022). While another 20% selected concerns about other legal risks, most still cited “not relevant to our business” (60%) as the primary reason for not using such data.

**ACTION:** Using biometrics? Now is the time to mitigate potential litigation risk – particularly in the US, as the success of the *Rogers* BIPA class action suit could encourage others to pursue their own claims.
The majority of respondents who are using or planning to use biometric data report collecting such information via fingerprints (53%). Other use cases include facial recognition (34%), voice recognition (32%) and iris recognition (28%).

Yet substantial numbers of respondents are currently, planning or considering using more invasive origination sources, such as heartbeat (8% using, 8% planning to use in the next year, 24% considering), ear shape (8% using, 6% planning to use in the next year, 37% considering) and even brain waves (5% using, 6% planning to use in the next year, 18% considering). Respondents that reported current usage of such data mainly hail from the technology industry, but usage of one or more of these was also reported by respondents from the construction, education, financial services, manufacturing and transportation industries.

Uses of such data tend to involve logging into or certifying payment through various apps, with top responses including initial identification or authentication, payment and other security functions. Fewer are using it for employee tracking or monitoring purposes, such as clocking in/out, employee onboarding and attention/focus detection of employees. More UK respondents are using biometrics for security functions, while more US respondents are using this data for clocking in/out and reading customer emotions.
What is your company’s status when it comes to biometric data originating from each of the following?

- FINGERPRINTS: 53% (CURRENTLY USING), 12% (PLANNING TO USE IN THE NEXT YEAR), 16% (CONSIDERING), 21% (NOT CONSIDERING AT THIS TIME)
- FACIAL RECOGNITION: 34% (CURRENTLY USING), 19% (PLANNING TO USE IN THE NEXT YEAR), 27% (CONSIDERING), 19% (NOT CONSIDERING AT THIS TIME)
- VOICE RECOGNITION: 32% (CURRENTLY USING), 16% (PLANNING TO USE IN THE NEXT YEAR), 19% (CONSIDERING), 32% (NOT CONSIDERING AT THIS TIME)
- IRIS RECOGNITION: 28% (CURRENTLY USING), 18% (PLANNING TO USE IN THE NEXT YEAR), 31% (CONSIDERING), 24% (NOT CONSIDERING AT THIS TIME)
- RETINA SCAN: 25% (CURRENTLY USING), 16% (PLANNING TO USE IN THE NEXT YEAR), 29% (CONSIDERING), 31% (NOT CONSIDERING AT THIS TIME)
- FINGER/HAND VEINS: 24% (CURRENTLY USING), 14% (PLANNING TO USE IN THE NEXT YEAR), 28% (CONSIDERING), 35% (NOT CONSIDERING AT THIS TIME)
- HAND GEOMETRICS: 23% (CURRENTLY USING), 11% (PLANNING TO USE IN THE NEXT YEAR), 31% (CONSIDERING), 35% (NOT CONSIDERING AT THIS TIME)
- EAR SHAPE: 8% (CURRENTLY USING), 6% (PLANNING TO USE IN THE NEXT YEAR), 37% (CONSIDERING), 49% (NOT CONSIDERING AT THIS TIME)
- HEARTBEAT: 8% (CURRENTLY USING), 8% (PLANNING TO USE IN THE NEXT YEAR), 24% (CONSIDERING), 60% (NOT CONSIDERING AT THIS TIME)
- SIGNATURE: 6% (CURRENTLY USING), 9% (PLANNING TO USE IN THE NEXT YEAR), 26% (CONSIDERING), 59% (NOT CONSIDERING AT THIS TIME)
- BRAIN WAVES: 5% (CURRENTLY USING), 6% (PLANNING TO USE IN THE NEXT YEAR), 18% (CONSIDERING), 71% (NOT CONSIDERING AT THIS TIME)

How is your company using or planning to use this data?
(Select all that apply)

- FOR INITIAL IDENTIFICATION OR AUTHENTICATION PURPOSES ONLY: 52% (US), 54% (UK)
- COLLECTING AND STORING FOR FUTURE PURPOSES: 52% (US), 49% (UK)
- FOR PAYMENT PURPOSES: 49% (US), 52% (UK)
- FOR OTHER SECURITY FUNCTIONS: 47% (US), 53% (UK)
- CLOCKING IN / CLOCKING OUT: 23% (US), 16% (UK)
- READING CUSTOMER EMOTIONS: 22% (US), 15% (UK)
- EMPLOYEE ONBOARDING: 14% (US), 17% (UK)
- ATTENTION / FOCUS DETECTION OF EMPLOYEES: 11% (US), 9% (UK)

Global Data Privacy Law Survey Report July 2023
Which of the following represent concerns for your organization with regard to specific restrictions on the collection and usage of precise consumer geolocation data? (Select all that apply)

- 51% SECURING CONSENT FROM CONSUMERS TO GATHER AND APPLY THIS DATA
- 56% DEFINING THE SPECIFIC BUSINESS PURPOSE FOR DATA APPLICATION
- 50% FACING ENFORCEMENT ACTIONS IF FOUND TO NOT BE IN COMPLIANCE
- 55% FACING LITIGATION
- 45% LOSING THE INSIGHTS THAT GEOLOCATION DATA HAS PROVIDED
- 36% LOSING THE REVENUE THAT GEOLOCATION DATA HAS PROVIDED
- 26% US
- 24% UK

Geolocation data raises concerns

Each of the new US state laws includes something not previously seen in the country: “a special set of extra protections for sensitive data,” says Claypoole. For many states, this sensitive data includes geolocation.

Meanwhile, the FTC is ramping up its enforcement efforts, such as a recent suit against an Idaho-based data broker alleging that it sold precise geolocation data associated with hundreds of millions of mobile devices.

It’s no wonder, then, that 40% of US respondents (versus 32% in the UK) are very concerned about privacy laws that include specific restrictions on collecting and using precise consumer geolocation data for targeted marketing purposes. US respondents are unsurprisingly also more concerned about enforcement actions (55% versus 45% of UK respondents) and litigation (50% versus 36%).

UK respondents, meanwhile, are more concerned about securing consent from consumers (56% versus 51% of US respondents) and defining the specific business purpose (55% versus 50%) – which tracks with their experience with the GDPR’s rights-based principles.

Finally, US respondents placed more focus on losing the insights that geolocation data provides (35% versus 26% of UK respondents), as well as associated revenue (24% versus 22%). This follows a consistent trend in which US respondents tend to prioritize monetization, whereas in the UK, the relative maturity of the GDPR may have created a more concrete foundation for individual rights and transparency.
To what extent is your organization concerned about privacy laws that include specific restrictions on collecting and using precise consumer geolocation data for targeted marketing purposes?

US

- **Very Concerned**: 40%
- **Moderately Concerned**: 42%
- **Slightly Concerned**: 14%
- **Not at All Concerned**: 4%

UK

- **Very Concerned**: 32%
- **Moderately Concerned**: 37%
- **Slightly Concerned**: 25%
- **Not at All Concerned**: 6%
Conclusion:
Preparing for the Year Ahead
Conclusion: Preparing for the Year Ahead

As our survey shows, complying with data privacy laws is no small feat – particularly given the evolving nature of not only the laws themselves, but the types of data collected via new technologies.

In this way, compliance itself is a moving target, and must be treated as such. That means, first and foremost, having a dedicated team in place – composed of information technology, human resources, legal, project management and other necessary departments – and ensuring they’re equipped with proper resources from leadership.

It also means that prioritization is key.

“Ultimately, data privacy compliance is manageable,” Claypoole says. “You don’t need to be perfect, but you do need to make the effort.”

Data Privacy Compliance Checklist

Follow these best practices to prepare for evolving data privacy laws:

- Designate an internal project manager or owner
- Establish a dedicated, multidisciplinary team that includes IT, HR, legal, compliance, marketing and engineering
- Conduct data mapping and understand data practices across the organization
- Develop platforms and systems to process and respond to data privacy rights requests
- Engage outside legal counsel to advise on compliance, particularly related to the 2023 changes and horizon scanning for subsequent years
- Update company privacy policies
- Plan and conduct data impact assessments
- Set metrics and specific goals to track compliance progress
- Draft or update agreements with third parties to comply with new privacy requirements
- Conduct a comparison of state privacy law frameworks to develop an agile compliance posture
Methodology and Demographics

In April and May 2023, Womble Bond Dickinson conducted a survey of 205 business leaders, representing 22 industries, who play either a leading or supporting role on data privacy issues. Half of these respondents (51%) were based in the US and represented 33 states. Forty-seven percent of respondents were based in the UK. Nearly half of the organizations surveyed stated that they have offices in the EU, with 25 different countries selected.

All responses were anonymous, and data has been analyzed in the aggregate.
Industry

- Technology / Telecom / Software: 17%
- Retail: 15%
- Financial Services / Banking: 14%
- Energy / Critical Infrastructure: 10%
- Manufacturing: 10%
- Healthcare / Life Sciences: 8%
- Construction: 5%
- Transportation / Distribution / Logistics: 4%
- Education: 3%
- Other: 15%

Company Headquarters

- United States: 51%
- United Kingdom: 47%
- South Africa: 1%
- European Union: 1%

Global Data Privacy Law Survey Report July 2023
Nature of Business Transactions

- Domestic (Home Market): 30%
- Multinational: 40%
- Mainly Domestic, Some International: 30%

Markets Where Company Does Business

- US: 64%
- UK: 57%
- EU: 38%
Privacy and Cybersecurity Team
Overview

Led by accomplished data privacy practitioners, including a certified legal specialist in Privacy and Information Security Law, Womble Bond Dickinson’s Privacy and Cybersecurity Team leverages deep knowledge and experience across the broad spectrum of privacy and cybersecurity legal issues.

Our transatlantic team of more than 40 attorneys provides privacy and cybersecurity legal guidance to clients in a broad range of sectors, including retail, financial services, healthcare, manufacturing, technology, education, telecommunications, government entities, and utilities. We counsel clients in the day-to-day privacy and cybersecurity issues affecting their businesses, and we also are trusted advisers should larger issues arise.

Core Services

- **Regulatory compliance and strategy.** We help clients identify and meet state, federal and international privacy regulations. The scope of our compliance practice includes data privacy, cybersecurity, marketing and advertising, international data transfers, and internet and telecommunications. We provide guidance to clients on the EU GDPR and UK GDPR, as well as CCPA, CPRA, HIPAA, COPPA, FERPA, TCPA, and FCC compliance and privacy obligations, along with other state and federal privacy, security and data breach laws.

- **Risk mitigation and data optimization.** We work to minimize legal and contractual exposure associated with these cybersecurity, data privacy and marketing restrictions and also help clients optimize data strategies and assist with IP licensing and data transactions.

- **Data breach planning and response.** We work with company leaders to craft response plans and train team members to respond to data breaches and other privacy-related crises. We also act as breach coach to entities suffering from data exposure incidents, ransomware attacks, wire fraud and/or other cyberattacks involving technology.

- **Government investigations.** We help clients manage responses to regulatory or criminal inquiries.

- **Data privacy and security disputes.** We protect our clients’ interests in court or before government agencies. We also advise clients on internet marketing, brand protection and complex domain name disputes.

- **Transaction data contracting and diligence.** We analyze data use limitations and information protection in contracts and M&A diligence reviews.

- **Digital marketing and advertising compliance.** We guide companies on social media issues, including use of influencers, text messaging, targeted advertising, giveaways and sweepstakes.