Thomson Reuters™

Fact Gathering for In-House Privacy Counsel

by Michael Hamilton, Adobe, and Michael Signorelli, Venable LLP, with Practical Law Data Privacy & Cybersecurity

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-048-3078**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

A Practice Note that discusses the critical but often underappreciated role of fact gathering for in-house privacy lawyers. This Practice Note explains how obtaining high-quality facts about a product, service, or technology is an essential first step for applying relevant law and delivering practical, actionable advice. It outlines the benefits of a thorough fact-gathering process, including enabling tailored legal application and facilitating informed risk decisions. This Practice Note details the key facts to gather regarding data collection, use, and security when conducting privacy impact assessments (PIAs). It also provides a step-by-step framework for the fact-gathering process, from initial engagement to final agreement on facts and legal analysis. By prioritizing rigorous fact-gathering, privacy teams can become more impactful strategic partners, supporting innovation while reducing the company's overall legal and regulatory risk under evolving privacy laws and regulations.

This Practice Note discusses a critical but underappreciated aspect of an in-house privacy lawyer's job: fact gathering. Obtaining high-quality facts about the product, service, technology, or system at issue and applying relevant law to those facts is an essential skill for the in-house practitioner. High-quality facts enable privacy teams to deliver more practical, applied advice, which leads to more options for the business. Privacy teams that focus on facts will play a more impactful and positive role within the business and reduce overall legal and regulatory risk for the company.

By contrast, if facts are not well-developed, counsel can only provide general legal guardrails for product and business teams. However, this advice is not actionable since business teams need to understand how the law applies to their specific activity. The best way to get to a useful and specific application of law is to first focus on thorough factual development.

This Note addresses fact gathering in the context of reviewing new products, features, services, or technologies (collectively, products) and assumes the company conducts its privacy legal analysis by performing privacy impact assessments (PIAs).

This Note discusses:

- The benefits and business case for thorough fact gathering.
- Details about the teams to involve, key facts to collect, and a step-by-step approach to fact gathering.
- Practical takeaways for privacy practitioners and in-house counsel.

Privacy Impact Assessments (PIA)

A PIA is a legal review focused on privacy issues. PIAs help organizations proactively understand and address privacy issues by analyzing the product's collection, generation, use, and storage of personal information.

PIAs form a cornerstone of effective privacy by design programs and provide many benefits, including:

- Identifying potential privacy issues early in the development process, when system redesigns or revisions may prove easier.

- Mitigating risks, which can lead to:
  - reduced personal information data breach costs;
  - avoiding potential reputational harm or adverse publicity; and
  - improved customer relationships and trust.
- Demonstrating and documenting compliance with privacy laws.
- Increasing privacy awareness within the organization.
- Ensuring consideration of the customer's or end user's perspective during the development process.

A growing number of state consumer data privacy laws require businesses to conduct PIAs, also referred to as data protection assessments (DPAs), when processing activities present a heightened risk of consumer harm or under other specified circumstances.

For more information on:

- PIAs, see Practice Note, Conducting Privacy Impact Assessments.
- Privacy by design programs, see Practice Note, Identifying Data Protection Issues for a New Product or Service and Using Privacy by Design Principles Checklist.
- US state consumer privacy laws, see US State Consumer Privacy Laws Toolkit.

Benefits of Thorough Fact Gathering

Executing a thoughtful, thorough fact-gathering process as part of a PIA will pay dividends by:

- Enabling tailored application of law (see Tailored Application of Law).
- Facilitating informed risk decision-making (see Informed Risk Decisions).
- Increasing efficiency and reducing rework (see Increased Efficiency).

A well-executed PIA is not merely a compliance checkbox. It is a strategic tool that equips businesses with the knowledge to make sound decisions, reduce risk, and operate more efficiently.

Tailored Application of Law

Accurate, detailed, and complete facts enable counsel to tailor recommendations to a specific situation rather than defaulting to generic guidance. Privacy analysis with underdeveloped facts often reduces to a general recitation of a law or regulation, which product and business stakeholders rarely find useful. Stakeholders need actionable guidance that applies privacy laws directly to their product or business initiative and gives them a range of options. Thorough fact development makes that possible.

For example, suppose a marketing team wants to use mobile device signals to send "nearby store" push notifications. If facts show the app collects precise geolocation data and shares it with a third party for ad measurement, specific guidance could:

- Provide a draft of the user notice.
- Address opt-in and opt-out requirements, depending on user location.
- Help map this use case to the company's existing mechanisms to restrict processing of sensitive data.
- Identify types of facilities where geofencing is restricted.
- Provide necessary contractual language for sharing data with the measurement company.

Without specific facts, the advice would be more generic, such as "inform customers in the privacy policy that we collect location data, get user consent where required by law, and provide users with a method to withdraw consent for location data collection." This advice is not actionable or complete enough to mitigate the associated risk.

Informed Risk Decisions

Privacy counsel must work to help the business make fully informed decisions with an understanding of the legal, business, and reputational risks involved. A deep understanding and application of facts to law enables legal counsel to identify the risks specific to the product and work with the business to identify risk mitigation strategies before making a decision. This includes identifying which options carry a higher likelihood of risk, as well as risks that could result in unintended consequences or significant impact. For more on risk categories and assessing

risk, see Practice Note, Conducting Privacy Impact Assessments: Identify and Understand Potential Risks.

For example, suppose a company's marketing team proposes uploading hashed email addresses to a social media platform to build lookalike audiences. Suppose further that the list of email addresses includes customers who previously opted out of targeted advertising, the social media platform treats the upload as targeted advertising, and the audience includes residents of states with opt-out rights for targeted advertising. With this full picture, counsel can recommend that the marketing team exclude opted-out users before hashing, honor state-specific opt-out signals, limit the platform's use of the hashed email addresses to contractually permitted purposes with no enrichment or sharing, and document an internal assessment reflecting the balancing of benefits versus risks of this arrangement.

Increased Efficiency

A well-structured fact-gathering process will significantly improve efficiency throughout the PIA process and beyond. Investing early in a detailed, accurate understanding of how a product functions and processes personal data reduces the need for repeated context setting and follow-up work. A single, shared factual record with stakeholder signoff will enable counsel to focus their time on the legal analysis and recommended solutions rather than re-confirming basic information or resolving inconsistencies across documents and teams.

Thorough fact gathering will also help streamline interactions with other company departments and functions. A consolidated factual summary that clearly describes data elements, flows, involved vendors, and security measures can serve multiple purposes, for example, when the commercial contract terms are negotiated. Over time, these efficiencies can build into a repeatable process that accelerates product development and vendor onboarding while improving the quality of privacy reviews.

Finally, deliberate fact gathering will improve institutional knowledge. Consistent documentation of product facts, how they evolved, and how they informed privacy decisions creates a valuable internal resource that stakeholders can reference, update, and repurpose. This reduces the burden on product, engineering, and legal teams, especially when onboarding new team members, responding to regulatory inquiries, and addressing customer questions.

Fact-Gathering Context

Teams Involved

The following groups and people are often involved in the fact gathering process, depending on the company size, industry, and other factors:

- **Product and engineering.** Product and engineering teams are responsible for launching new products, features, and services and have expert knowledge on product issues. They are also responsible for addressing any guidance in the PIA, such as suggested changes to product functionality.
- **IT.** A company's IT group may work directly with the product and engineering teams on how the product the company is developing or purchasing will integrate with the company's network, systems, and data. They will be able to provide key information about data flows and security measures.
- **Procurement.** Larger companies usually have dedicated procurement teams that run the process of evaluating potential third-party vendors, understanding the product at issue, and negotiating vendor pricing and terms. They may play a role, along with the business groups they support, in understanding the facts surrounding the purchase and how the product functions and integrates into the company's systems.
- **Product counsel.** Some organizations, such as technology companies, have a dedicated product lawyer who supports specific products. These lawyers have in-depth product knowledge and serve as the primary legal contact for product and engineering teams. Other organizations take a business partner approach, where each counsel supports certain business groups or functions and is familiar with everything those clients do, not just the products they develop.
- **Privacy counsel.** Many larger companies have a dedicated team with subject matter expertise on privacy. This team is responsible for monitoring global privacy developments and advising the company on how to address them. Privacy counsel works closely with product counsel; in some organizations they may be part of the same

larger team or the privacy and product counsel roles may be combined. A privacy lawyer's value stems from their legal expertise paired with a strong understanding of the relevant technology and business imperatives, enabling the lawyer to provide tailored and practical guidance to the product team that enables them to achieve their goals while addressing privacy laws and customer privacy expectations.

- **Outside legal counsel.** Outside counsel brings a deep expertise in the law and robust experience across different clients and industries to help guide the fact gathering, analysis, and overall PIA process. If outside counsel is involved, their work product will be more valuable if it is applied to a discrete set of facts. To help save on outside counsel fees, in-house counsel may perform the initial fact gathering exercise and ask outside counsel to help propose follow-up questions for the product or business group or assist in the PIA legal analysis and risk mitigation strategies.

Key Facts

Fact gathering is the process of ascertaining all relevant details of the product that the company is developing, enhancing, or purchasing. At core, the facts are the details of what product does, what data it collects, how it uses the data, how it secures the data, and what third parties are involved. Facts are designed to answer and provide details on the following questions:

- **What business problem does the product intend to solve?** It is essential for counsel to understand why the company is developing or purchasing the product and how it fits into their broader strategy or business goals.
- **What data will the product collect?** It is usually unhelpful to ask product teams an open-ended question about whether they collect personal data. Business teams may not appreciate the breadth in scope of privacy laws or understand terms like personally identifiable information, sensitive personal data, pseudonymized data, or deidentified data. Instead, counsel should gather data from product and business teams at the granular, data element level. Counsel can then assess whether such data is in scope with how applicable laws define personal data. For more information, see Practice Note, Conducting Privacy Impact Assessments: Identify System's Personal Information.
- **What is the source of the collected data?** Examples of data sources include user-generated content, user-provided information, data collected via digital tracking technologies, data purchased from third parties, or data pulled via an API. Counsel should also identify whether there are restrictions imposed on the source data such as customer instructions or data provider agreements.
- **How will the product use the collected data?**Counsel must ascertain all initial and anticipated future uses of the data collected through the product. Asking the product team about their long-term roadmap and goals may help identify future uses. Counsel should also address whether the product will generate or derive new data from the collected data, whether it uses or relies on automated decision-making or profiling technology, or train AI models.
- **How will the product store and retain the collected data?** Counsel must determine how and where the company will store the data the product collects, for example, in a public or private cloud or on premises servers. They also must assess how long the company plans to retain this data, whether these plans comply with any retention policies, and whether deletion will be automatic or manual when the retention period expires.
- **Will the product share, transfer, or disclose the collected data?** Counsel must establish the company's plan to share, transfer, or otherwise disclose the data the product collects. It is important to ask this question in different ways to truly ascertain if data will fall under a particular law's definition of data sharing or a data transfer. For example, allowing another party to access the data through its own login to the company's system could be considered a data transfer under certain laws. Counsel should also ask whether any data will be transferred to or accessed from a location outside the US or transferred from an international location into the US.
- **How does data flow through the product?** Determining the data flow through a product usually involves documentation in both narrative format and visual diagrams or maps. Visual aids are especially helpful when discussing the details of the data flow with the product and engineering teams. For example, during a whiteboarding exercise counsel or another participant can draw a data map and easily add, change, or erase sections depending on the answers to questions, and record any outstanding items that require follow-up to

complete the data flow. For more information, see Practice Note, Conducting Privacy Impact Assessments: Describe Information Flows.

- **What is the role of any vendors or third parties in the product?** Products often include technology from vendors. Mapping the data flow through the product should indicate where vendors or other third parties are involved. The vendor should provide robust documentation around their product offering. For more information on vendor management, see Practice Note, Managing Privacy and Data Security Risks in Vendor Relationships (US) and Managing Vendor and Service Provider Cyber Risks Toolkit (US).
- **What is the product output?** Counsel should review a typical output from the product. For example, will the product issue an aggregated report to customers or an internal team, generate recommendations to customers, or provide chatbot responses to employee questions? Reviewing the output will assist counsel in identifying any additional data elements, use purposes, data minimization opportunities, and follow up questions about the product.
- **In what states and countries will the product be offered, accessed, or used?** Determining where the product will be deployed, accessed, sold, and used will inform the privacy risk and scope of privacy analysis. For example, if a product will only be made available to customers in the US, then the PIA will generally not need to address EU or UK legal requirements.
- **What technical and organizational measures will secure the product?** Counsel must determine, with the help of the IT security team, the technical and organizational measures in place to secure the product and the data it contains. Does the product employ hashing, encryption, differential privacy, or other privacy enhancing technologies (PETs)? Counsel should give special consideration to whether the product will integrate with the organization's security stack and if the appropriate security team has reviewed it and identified any risks or gaps. For more information on cybersecurity and information security, see Practice Note, Cybersecurity Issues for In-House Counsel (US), Information Security Toolkit, and Cybersecurity Toolkit (US).
- **What contract terms are in place or proposed?** Counsel should review the contract terms in the product purchase, sale, or licensing agreement to identify any gaps in privacy and security language and each party's related obligations, indemnity, liability, and other key terms. This may involve working with the attorney responsible for the commercial contract terms depending on the company size or structure. For more information on contract language, see Standard Clauses, Data Security Contract Clauses for Service Provider Arrangements (Pro-Provider) and Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer).

Fact Gathering Process

This section outlines the five primary steps of fact gathering:

- Initial engagement (see Initial Engagement).
- Factual development (see Factual Development).
- Final agreement on facts (see Final Agreement on Facts).
- Privacy legal analysis (see Privacy Legal Analysis).
- Updates to facts (see Factual Updates).

These steps will vary by company but form a general framework for the fact gathering process.

Initial Engagement

Initial engagement starts with the product team or relevant business group initiating the PIA in line with the company's standard process, perhaps in coordination with product counsel. Product teams may start by answering a basic set of questions about the product at issue (see, for example, Standard Document, Threshold Privacy Review).

At all stages of the fact-gathering process, counsel should work to minimize the burden on product teams by, for example, asking teams to provide links to existing documentation rather than create new documentation in a different format for the PIA. Nonetheless, product teams should answer a basic set of questions to initiate the review process.

Counsel should also guide the business on the best time to initiate a PIA. This should not take place so early such that the product and engineering teams haven't fleshed out the details on the product's design and operation. A good test is whether counsel can answer the basic factual questions described above. If not, it may be too early to initiate privacy legal review. However, the PIA should not occur so

late such that all product and engineering decisions have been finalized and legal does not have a real opportunity to provide input on the product and suggest privacy mitigations.

Factual Development

Factual development is the most interactive step of the fact gathering process. Legal counsel, product and engineering teams, business groups, IT, and outside counsel (if engaged) do the hard work of identifying, distilling, and summarizing the key facts and asking follow-up questions to fill in details and gain clarity. The goal is to document a set of facts that is concise, detailed, and comprehensive.

Holding an initial kickoff meeting between the product and legal teams to discuss the goals of the product, timing, initial questions, key documentation, and planned next steps will help set proper expectations and ensure all parties understand the fact-gathering and PIA process.

The product team or the business team purchasing the product should be able to provide information on the key facts of the product, such as data collection and flows, the vendors involved, and integrations with a company's systems. This point person is also the overall driver on the product launch, deployment, or engagement, and they provide the impetus and drive for completing the privacy legal review.

Based on the documentation provided and verbal conversations, product counsel and privacy counsel can start drafting a factual summary in narrative form, working towards an agreed-upon set of facts. This drafting will typically require back and forth with product and other teams as legal teams review the documentation and ask follow-up questions. If outside counsel is involved, they may have additional questions and insights that will help flesh out the facts section.

The level of factual detail will depend on the complexity of the product, the amount and type of personal data involved, and whether the product is a new launch or a product update.

Final Agreement on Facts

After product counsel and privacy counsel have prepared a complete summary of facts, product and engineering teams should conduct a final review of the document and validate that the facts are accurate and complete.

Privacy Legal Analysis

Once the facts have been finalized, privacy counsel can proceed to the privacy legal analysis. By starting with a robust set of facts, this analysis can be a nuanced and practical application of the law to the facts.

If the company has engaged outside counsel, it will be most efficient to seek and receive their input on a final set of facts. In addition to deep understanding of the law and close engagement with regulators, outside counsel often brings a bird's eye view of developments in a particular industry or jurisdiction and has the cumulative experience of applying the law to many different factual scenarios for a variety of clients.

Factual Updates

Products, services, and technology are not static, but are regularly updated to stay current and competitive. Thus, facts will change that may impact the legal analysis over time. Striking a balance between rigidity and flexibility in the fact-gathering process is key to accounting for the realities of fast-moving technology landscape.

One approach is to build enough flexibility into the facts as described such that the business teams have freedom to operate within that context. This could mean upleveling the facts so that instead of describing an item on a very specific level, such as the particular encryption methodology a product employs, the facts are set out at a higher level, for example, stating that the product will employ a standard encryption framework. While the legal analysis will not be as tailored, product teams will have more flexibility.

The second approach involves asking product and engineering teams to forecast potential future changes and developments during the fact-gathering process. Counsel can ensure that guidance on these changes is built into the PIA, which will save all parties time if the changes come to fruition.

Despite using one or both approaches, there will inevitably be times when the facts change and require updates to the final fact description and the resulting PIA. Product counsel should check in regularly with the business to identify any changes, iterations, or developments in the product that may necessitate these updates. Many organizations regularly review their privacy assessments and

make updates as necessary to reflect changed circumstances and facts.

Monitoring for Legal and Regulatory Changes

The legal and regulatory environment is constantly evolving to address new and developing technologies. Privacy counsel must recognize that new laws, regulations, regulatory guidance, and enforcement trends may impact existing PIAs. A product that was low risk when first launched may become higher risk if, for example, a new state consumer data privacy law comes into force, a regulator issues guidance on a particular technology, or an industryspecific rule expands its definition of sensitive data.

Working Towards Partnership

Thorough and detailed fact gathering lays the necessary foundation for a meaningful privacy analysis and an efficient PIA process. High-quality, well-organized facts enable privacy counsel to deliver concrete, tailored recommendations that product and business teams can understand and implement. When privacy teams understand how a product functions, how it processes personal data, and its role in the company's broader strategy, they can more readily identify risks, propose mitigation options, and support the business in achieving its objectives. This will position privacy teams as strategic partners in product development and innovation while reducing overall legal and operational risk.

Counsel should work to improve their interview skills and develop their confidence in conversing with product teams. When counsel can learn to "speak the language" of the product teams they support, the process becomes more collaborative and each successful fact-gathering exercise helps to build a partnership with clients. Ultimately, privacy teams that prioritize rigorous fact gathering will become more impactful and trusted partners to the business.