ROTHWELL FIGG
IP Professionals

SPRING CLEANING WHILE YOU ARE HOUSEBOUND

5 STEPS TO BETTER DATA PRIVACY HYGIENE

Image Source: http://cliparts.co/cleaning-retro

Privacy
Data Protection
Cybersecurity

STEP ONE: DATA MAPPING

The first step for cleaning up your data practices should always be data mapping. Think of this as the 'pull everything out of the closet and see what you've got' step. And keep in mind, as with a lot of cleaning, the mess may look bigger once you pull it all out—but try not to get overwhelmed.

What. The goal of data mapping is to determine what *personal information* (e.g., name, address, email address, telephone number, health data, financial data, IP address, location information, etc.) your organization stores. While personal information is defined differently under different statutes, it is best to not data map with any particular statute in mind, but rather, to just have an *extremely broad* understanding. This will ensure that nothing falls between the cracks.

How. There are different ways to figure out what personal information your organization stores, including talking to relevant people (e.g., operations, HR, records and information management, IT, marketing, finance, webpage design, legal), exploring saved files, and exploring any consumer interfaces or platforms the company uses to engage with consumers.

Where, Who and When. In addition to inventorying what data you have, you also want to track where and how the data is stored and who has access to the data. And if any of the information is de-identified, or aggregated, that is also worth noting.

"Think of this as the 'pull everything out of the closet and see what you've got' step. And keep in mind, as with a lot of cleaning, the mess may look bigger once you pull it all out—but try not to get overwhelmed."

Use. It may also be useful to determine when the data was obtained; when it has been used by the organization; and how it has been used by the organization. This may include any instances of sharing or selling the data to third parties.

Why. There are several goals of data mapping:

(1) Determine what you have that you do not need. Like all spring cleaning, you will likely throw some stuff out. This may include getting rid of "stale" data or data that you once collected, but have not used (like a piece of clothing you bought six years ago, seemingly love, but have yet to find an occasion to wear it).

(2) Rearrange what you have so it is more organized and readily accessible going forward.

(3) Create a "map" of your data flows, detailing what data you have, where it is stored, how it is stored, who has access to it, how often it is deleted, and how it is used (including shared/sold).

(4) Communicate the map to others in the organization and have them confirm accuracy. Calendar periodic updates to check that the map continues to properly reflect the organization's management and storage of data.

STEP TWO: ASSESS YOUR PRIVACY FRAMEWORK

A second step in data spring cleaning is to assess your legal obligations and business plans. Think of this as making a list of what you *need* to have in your closet, and then cross-checking what you need with what's already there. We recommend three sub-steps in assessing your company's privacy framework: (A) contract review; (B) business plans/initiatives review; and (C) data privacy and security law review.

A. CONTRACTS

The first step in a contract review is gathering together all relevant contracts (e.g., contracts with business partners, vendors, and customers). The contracts should then be reviewed to determine:

Obligations. What obligations do the contracts impose on the organization with respect to data management, privacy, and security?

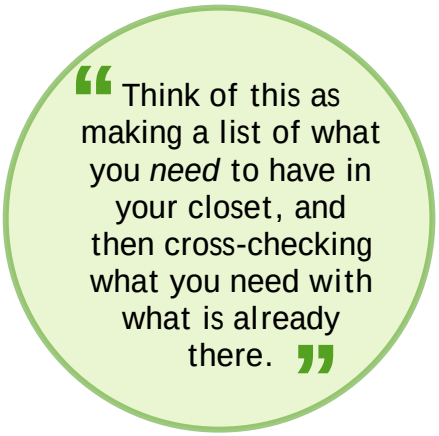
Data use. What does the contract say regarding the sources of the data, nature of the relationship, and how the data is being or can be used?

Data ownership. Does the contract speak to data ownership or the value of the data for purposes of data analytics and advances in artificial intelligence and machine learning?

B. BUSINESS PLANS/INITIATIVES

In addition to assessing contracts that are already in place, it is important to talk to individuals with relevant information concerning:

- contracts that are in the negotiation process;
- business plans and initiatives;
- sales plans and initiatives;
- engineering plans; and
- big data/data analytics/data science plans.



Ultimately, you will want to ask: does the personal information that we collect and use align with our business goals and contractual obligations?

C. DATA PRIVACY AND SECURITY LAWS

After evaluating the organization's data and contracts, and assessing current corporate efforts, plans, and goals, it is a good time to assess what data privacy and security laws apply to your organization. By referring to your data map, you can see the categories of data you collect and determine whether that data falls within the scope of protected personal information under federal and state privacy law. In general, an organization that tried to be compliant with applicable laws will fare better—should an issue arise—than one that did not try. Rothwell Figg is available to help you with Step Two (or any other step), should you need help.

STEP THREE: PLAN FOR BACK-END SYSTEM CHANGES

The third step of the spring data cleaning process asks organizations to consider which behind-the-scenes changes need to be made to implement a secure and compliant data privacy management system, with protocols to check vulnerabilities and to avoid security breaches and data leaks. We provide below a list of server-side updates that your company may wish to consider for sprucing up the back of house. For a more complete list, consult the list you made in Step Two… anything not checked off as already being on your data map is a "to do" item.

Reasonable security. Do you have reasonable security measures in place for each point on your data map? Have you taken into account potential vulnerabilities with individuals (e.g., employees) and IT assets (hardware and software)? It is critical to maintain documentation of any data security procedures to demonstrate compliance and, if needed, to defend your company's activities in a litigation or enforcement action. See Example A below for a more detailed look at how to implement reasonable security.

Data subject requests. If applicable to your company, do you have mechanisms in place for receiving data subject requests to access, modify, delete, disclose to third parties, or opt-out of the sale of their personal information (e.g., toll-free telephone number, website submission form, a "Do Not Sell My Personal Information" link, and/or email address)? And do you have a proper identity verification process to authenticate the identity of those consumers making such requests? See Example B below for a more detailed look at what you need for data subject requests.

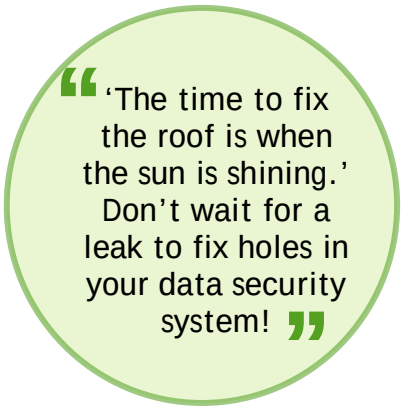
Non-Discrimination. Does your business charge different prices or rates, or offer discounts/incentives or a different level of quality of service, to those consumers who exercise their rights to access/modify/delete/disclose/opt-out of the sale of their personal information? Under some laws (e.g., CCPA), some price, quality, or service differences are ok if such a difference: (1) is directly or reasonably related to the value of the consumer's data; and (2) does not result in unjust, unreasonable, coercive, or usurious financial incentive practices.

Data transfers. Is the data that your company collects and uses in a form that is readily transferrable and portable? Do you have an appropriate mechanism in place for facilitating cross-border data transfers? Acceptable options for international data transfer may include:

- Privacy Shield (e.g., an adequacy scheme where another nation's privacy rights and regulations are deemed "essentially equivalent" to those ensured within the transferee nation);
- Standard Contractual Clauses that have been approved by a supervisory authority;
- Binding Corporate Rules for intra-organizational cross-border transfers that must be pre-approved by a supervisory authority;
- Enforceable codes of conduct and approved certification mechanisms (e.g., industry standards for demonstrating data security); and
- An applicable derogation (e.g., consumer consent, legal need, or public interest- rare and must meet a high bar).

STEP THREE EXAMPLE A: REASONABLE SECURITY

Under the CCPA, a business must implement "reasonable security procedures and practices." The GDPR has a very similar standard, requiring companies to provide "appropriate" technical, physical, and administrative controls to protect personal information. While this "reasonableness" standard is notoriously vague, and may depend on, e.g., the scope of the business's activities, the sensitivity of the data collected and used, and the size of the company, there are recognized standards (e.g., the NIST Cybersecurity and/or Privacy Frameworks) and general best practices that should be explored and implemented when possible:



Data Minimization. Less is more. Simplify your data management and minimize risk by only collecting and processing that data which is necessary for a legitimate business purpose and keep this data for no longer than is necessary for carrying out such purpose (and ensure secure destruction once the data is no longer needed).

Data Integrity and Confidentiality. Your company should consider technical, physical, and administrative access controls to minimize potential vulnerabilities across all facets of your data security system:

- Integrate data privacy into an information security policy;
- Maintain policies/procedures for the de-identification, encryption, and/or aggregation of personal data (with strong and up-to-date algorithms);
- Maintain technical security measures (e.g., intrusion detection, firewalls, monitoring);
- Maintain procedures to restrict access to personal data (e.g., role-based access);
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets) and use of information resources policy;
- Maintain HR security measures (e.g., pre-screening, performance appraisals); and
- Maintain a security certification (e.g., ISO).

Data Breach Response. "The time to fix the roof is when the sun is shining." Don't wait for a leak to fix the holes in your data security system! Your company should have in place an effective data privacy incident/breach response plan to contain and recover from a data breach, and to ultimately help your company with serious damage control and to stave off hefty penalties and fines. For an effective data breach response, your company should:

- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol;
- Maintain a log to track data privacy incidents/breaches;
- Monitor and report data privacy incident metrics (e.g., nature of breach, risk, root cause);
- Conduct periodic testing of data privacy incident/breach plan; and
- Obtain data privacy breach insurance coverage.

STEP THREE EXAMPLE B: DATA SUBJECT REQUESTS

Having now categorized the data that aligns with your business goals and legal obligations, your business may wish to (or be legally required to) implement a process for retrieving this data upon request. Like needing to find your ugly holiday sweater, or those spices at the back of your pantry, your business needs a plan for how to manage individual consumer data, such that it is easy to find and readily accessible/modifiable when needed.

Under the CCPA, consumers have the right to access, request disclosure, delete, and opt-out of the sale of their personal information. It is likely that other states will follow in California's footsteps in the years to come. In view of this, your business should consider whether or not it should set up the infrastructure to accept and respond to data subject requests.

"Like needing to find your ugly holiday sweater, or those spices at the back of your pantry, your business needs a plan for how to manage individual consumer data, such that it is easy to find and readily accessible/modifiable when needed."

Mechanisms for receiving data subject requests may include, depending on the applicable law:

(1) a toll-free telephone number;
(2) a website submission;
(3) an email address; and/or
(4) a "Do Not Sell My Personal Information" link (e.g., CCPA opt-outs).

Verification: The established submission methods should provide secure portals for managing user requests, and each data subject request must be verified to authenticate the identity of the requesting consumer (e.g., though password/username, photo verification, security questions, access codes, etc.). The acceptable and recommended verification methods will be determined on a state-by-state basis, upon guidance from the state Attorney General.

Once the request submission mechanisms are in place, your company should develop standard data retrieval procedures, reporting formats, and a system to track requests and how/when those requests have been addressed. Creating customized workflows for your employees to follow with simple, easily followed procedures will ensure uniform management of users' requests. The procedures should allow for quick turnaround, with responses to consumer requests completed within about 45 to 60 days.

Know your limits: The requests must be reasonable (e.g., limited to two requests per person per year, and a response scope to the past 12 months). Furthermore, you may not have to agree to the request if the data use/collection is necessary for specific business, legal, or public interest purposes.

STEP FOUR: UPDATE PRIVACY POLICY, CORPORATE POLICIES, AND CONSENT FORMS

> "Transparency is the name of the game, so wipe down that window into your privacy practices and let consumers see exactly what data you collect and what you do with it."

Gone are the days of sweeping your "dirty" data practices under the rug! Those businesses being hailed as leaders in this new era of data privacy are those that proactively demonstrate accountability for consumer rights and seek explicit consent for data usage. Transparency is the name of the game, so wipe down that window into your privacy practices and let consumers see exactly what data you collect and what you do with it. Dusting off your privacy policy is a step in the right direction, along with updating any consent forms, cookie notices, and third party data transfer/service agreements.

Documentation that you should consider drafting and updating includes:

Privacy Policy. Update your privacy policy to comply with applicable laws, data practices, and business goals/plans. As a best practice, your privacy notice should be updated at least once a year and should contain at least: the categories of personal information collected, the categories of third parties with whom personal information is shared, a description of how to submit a data subject access request (if such process exists), and the effective date of the notice.

Authenticating Policy. Draft policies for authenticating individuals who make subject rights requests; who subject opt-in or opt-out requests; who submit "do not sell my personal information" requests; etc.

Written Information Security Plan (WISP). Memorialize security policies and procedures in a written security plan that conforms to industry standards.

Cookie Consent Pop-Up. This is required by GDPR and the EU e-Privacy Directive. It is not required under CCPA (though CCPA requires that a privacy policy include description of one's cookie policy), but it is a good idea to include a cookie policy.

Service Provider Agreements. Review service provider agreements to identify potential gaps with policies, and update agreements.

Data Transfer and Service Provider/Data Processing Policies. Consider whether one or more policies should be implemented regarding data transfers, and service provider/data processing requirements.

STEP FIVE: TRAINING AND COMPLIANCE UPKEEP

Like all cleaning, tidying up your data privacy practices for compliance is not a one-and-done task. In order to keep a "clean" house, your business will need to provide regular trainings and awareness programs to promote compliance with your privacy policies, and to mitigate operational risk. This is particularly true because – as with all things – staying organized and maintaining good data hygiene takes work. For example, employees will come and go (and need to be educated); new types of data will be collected as your business evolves over time; data storage and transmission practices will morph over time; the patchwork of state and federal privacy laws (each with ongoing requirements) will continue to evolve; new contracts will be entered into; and the list goes on.

Options for communicating privacy policies and training employees may include:

- Conducting a refresher training based on your updated data map, contracts, and legal obligations, data subject requests, and privacy policies;
- Incorporating data privacy into operational training (e.g., HR, marketing, call center);
- Delivering training/awareness in response to new state laws and regulations;
- Developing a privacy newsletter, or incorporating privacy into existing corporate communications;
- Providing a repository of privacy information (e.g., an internal data privacy intranet);
- Maintaining privacy awareness material (e.g., posters and videos);
- Maintaining scripts for use by employees to explain or provide the data privacy notice; and
- Conducting privacy awareness events (e.g., an annual data privacy day/week).

If you have not done so already, your business should establish a privacy governance structure:

- Identify those individuals who will be responsible for data privacy (e.g., a privacy office, a Data Protection Officer, general counsel) and maintain privacy qualifications/certifications; and
- Hold regular meetings and engage relevant stakeholders throughout the organization (e.g., operations, HR, records and information management, IT, marketing, finance, webpage design, legal).

Privacy Impact Assessment. Consider whether a privacy impact assessment should be conducted, to identify and document privacy risks and potential implications.

Security Risk Assessment. Consider whether a security risk assessment should be conducted, to identify and document security risks and potential implications.

AUTHORS

Privacy
Data Protection
Cybersecurity

Jenny L. Colgate and Caitlin M. Wilmot are members of Rothwell Figg's privacy, data protection, and cybersecurity team.

The team at Rothwell Figg helps clients understand and navigate the rapidly evolving areas of privacy, data protection, and cybersecurity law. We work with our clients to prepare, integrate, and implement compliance strategies, frameworks for risk management, and best practices. We have experience working closely with our clients to inventory their data and assess their legal obligations; to implement back-end and structural changes that are not only compliant, but also workable; to prepare written policies, assessments, forms, and notices to effectuate legal requirements and best practices; to negotiate, draft, and review agreements for compliance; and to help train staff. We can assist with the design and implementation of incident response plans, and if there ever is an incident, we can serve as trusted advisors, from the investigation stages through litigation, helping you navigate disclosure requirements to public authorities. Most of the attorneys in the practice group are experienced litigators with deep technical backgrounds, and have represented clients in multitudinous venues, including before numerous government agencies, and in state courts, federal district courts and courts of appeal, and the United States Supreme Court.

Jenny L. Colgate **Caitlin M. Wilmot**