Thomson Reuters™

Data Minimization and Avoiding the Over-Retention of Personal Information

by Martin T. Tully and Nick B. Snavely, Redgrave LLP, with Practical Law Litigation

Status: **Law stated as of 10 Dec 2024** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-037-0578**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

An Article explaining the risks and costs of an organization needlessly retaining personally identifiable information and digital records that have outlived their utility or business value and are digital debris. This Article identifies data minimization mandates, describes the risks organizations face when over-retaining personal or useless data, and explains how they may defensibly dispose of it.

Retaining personal data and other types of digital records that have outlived their utility or business value can present significant costs and risks to an organization. Counsel should take stock of the volume of useless data their organizational clients are needlessly storing and devise ways to dispose of it responsibly.

In particular, counsel should:

- Create a list of the various types of data and records the organization is storing, and derive from that a list of what it is unnecessarily storing.
- Establish a system for defensibly disposing of data the organization no longer reasonably needs.
- Implement a process for reducing the amount of digital debris unnecessarily retained in the future and periodically updating that process.
- Regularly review federal and state-specific regulations for changes to data collection, minimization, and disposition requirements (among others) that affect how (and for how long) companies retain personal information.

For resources to help in-house counsel and law firm attorneys manage an organization's records and other data, see the Records Management Toolkit and the Global Records Retention Toolkit. For more information on the responsible destruction of a non-profit organization's data, see Standard Document, Records Retention and Destruction Policy (Non-Profits).

The High Cost of Retaining Digital Debris

Data minimization and the routine, defensible disposition of data are essential to maintaining an organization's information hygiene. Some types of data are useful for only a short amount of time, while others, such as certain vital corporate records, may have a nearly infinite useful life. But the vast majority of data reaches a point after some time where it no longer has business value. When an organization retains data beyond its useful life, the primary question to ask when deciding whether to retain it is whether the business **can** extract value from it. The related question is whether the business **actually** extracts value from it. The likelihood that an organization accesses aging data decreases exponentially over time. The data eventually becomes digital debris, which industry experts commonly refer to as data that is redundant, obsolete, or trivial (ROT).

Companies often retain data by default regardless of its business value. Therefore, digital debris tends to accumulate indefinitely absent a company's affirmative steps to the contrary. Continued ownership of this debris is a significant and growing business expense at many organizations. Raw storage space may be cheap, but the total cost of owning enterprise data has increased due to the rising costs of security, labor, migration, maintenance, and other

factors. Even if the trend reverses, the trajectory of growing data volumes is unlikely to subside.

For more information about the cost of over-retention, see Article, Act Now or Pay Later: The Case for Defensible Disposition of Data: The High Costs of Data Over-Retention.

Regulatory Restrictions

The situation is worse than organizations needlessly spending money to retain digital debris. The unnecessary retention of personally identifiable information, protected health information, payment card industry data, and a host of other consumer, employee, and business information also exposes organizations to potential criminal, civil, and regulatory penalties. Until recently, most legislative and regulatory activity focused on the relatively established requirements of the records that organizations must keep, such as for tax purposes. However, regulators now additionally focus on the quickly evolving requirements of:

- The types of data that organizations may obtain and keep.
- How long organizations may keep different types of data.
- The various ways organizations must protect or dispose of this data.

Consequently, organizations not only spend money to store data that lacks value but may also perpetuate latent liabilities that grow more serious with time.

In this regard, the legislative and regulatory environment has shifted in the past several years. Spearheaded by new data privacy and cybersecurity mandates, organizations are increasingly restricted to:

- Collecting only the personal data they absolutely need.
- Using personal data only for the explicit purposes for which they collected it.
- Disposing of personal data appropriately as soon as they no longer reasonably need it.

(See The Advent of Data Minimization Mandates.)

Organizations that stray from these data minimization dictates do so at their peril. As a result, many organizations now view the defensible disposition of ROT, particularly personal data, with renewed interest and a sense of urgency.

The Rise of Defensible Disposition

Information governance is fundamentally a business function. The Supreme Court recognized that information governance is a business function when it observed that ordinarily, "it is not wrongful for a manager to instruct his employees to comply with a valid document retention policy, even though the policy, in part, is created to keep certain information from others, including the Government" (*Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005)).

Many other courts have likewise recognized that record retention policies serve important and legitimate business purposes (see, for example, *Spanish Peaks Lodge, LLC v. Keybank Nat. Ass'n*, 2012 WL 895465, at *1 n.3 (W.D. Pa. Mar. 15, 2012) (denying motion for spoliation sanctions based on evidence destroyed under a document retention policy, because credible testimony established that "the document retention policy was implemented for legitimate business purposes unconnected with the current litigation") and *Barnett v. Deere & Co.*, 2016 WL 4544052, at *4 (S.D. Miss. Aug. 31, 2016) (noting that "[t]he court does 'not draw an inference of bad faith when documents are destroyed under a routine policy'") (quoting *Russell v. Univ. of Tex.*, 234 Fed. App'x 195, 208 (5th Cir. 2007))). For more information on drafting a document retention policy, see Practice Note, Drafting a Document Retention Policy.

The primary purpose of an information governance program is to manage the organization's information in ways that meet the organization's legal and regulatory obligations. Simultaneously, the information governance program should contribute to the business's efficiency, productivity, and overall value. Digital debris impedes these efforts in many ways, such as by making it difficult for:

- Users to find the information they need when they need it.
- The organization to identify and extract benefit from a subset of valuable information.
- Compliance groups to mitigate risks related to the organization's prolonged retention of certain records.

The crux of most business decisions is the anticipated return on investment. This is, in other words, balancing expected value against expected

cost or risk to determine whether a task is sufficiently net positive to warrant proceeding. Decisions on retention and disposition of information are no different. Information has value, incurs cost, and can create or mitigate risk.

Reasonable Retention

Counsel should approach decisions involving data retention and disposition sensibly. The yardstick by which a regulator measures an organization's conduct is reasonableness. It considers what a typical organization acting with regular prudence does under similar circumstances. A regulator does not expect or require perfection because it is impossible. An organization's proposed initiatives to dispose of large volumes of ROT may otherwise be paralyzed due to concerns it may contain documents relevant to a future legal or regulatory proceedings.

Regardless of whether the organization can identify these documents related to a future proceeding, the regulator's question is not whether the organization applied a retention and disposition framework to keep every relevant bit or byte of relevant data. It instead examines whether the organization's processes were reasonable under the circumstances. The hallmarks of reasonableness include processes that are sensible, consistent, programmatic, and well-documented.

Reasonable retention is not an all-or-nothing proposition. The fact that it is neither practical nor possible for an organization to identify and purge all ROT does not mean that it cannot make significant gains using tactical initiatives targeting particular data stores. For example, an organization can achieve significant reductions in hard and soft costs simply by:

- Adopting a framework for classifying information it creates and receives (see Bifurcate Information).
- Remediating the organization's most readily identifiable and addressable ROT.
- Assigning conservative retention periods to the remainder of the organization's existing data so that it remediates the less readily identifiable ROT over time.

Bifurcate Information

Most organizations find it useful to bifurcate their information universe into already-existing information and newly created or received information.
Even an organization that cannot address the ROT in its existing information stores can make significant progress toward reasonable retention by developing and implementing a sound framework for the classification, retention, and disposition of information that it creates or acquires.

Bifurcating information and implementing the necessary policies, procedures, and technologies for the organization to retain and dispose of information helps it set a course that:

- Allows unclassified legacy information to age out.
- Manages current, properly classified information according to:
  - the organization's business needs; and
  - legal and regulatory obligations.

The Advent of Data Minimization Mandates

Defensible disposition and data minimization norms are becoming increasingly necessary for many organizations, especially for personal and sensitive data. In the past several years, jurisdictions within and outside the US have adopted regulations and requirements mandating data minimization related to privacy and consumers' personal information. While the details vary among jurisdictions, several have adopted mandates that boil down to the two basic concepts that companies must not:

- Collect more personal data than necessary to fulfill some legitimate purpose.
- Keep what they have collected any longer than necessary to serve that purpose.

General Data Protection Regulation (GDPR)

As with many aspects of privacy regulation, the European Union's General Data Protection Regulation (GDPR) led the way in data minimization (see Practice Note, Overview of EU General Data Protection Regulation). Article 5 of the GDPR lists six principles on how to process personal data, two of which directly address data minimization. Article 5 also requires for personal data to be:

- Limited to what is necessary for the purpose of processing the personal data.

- Retained in a way that allows data subject identification for only as long as necessary for the purpose of processing the personal data.

(GDPR Article 5(1)(c), (e).)

Recital 39 reiterates that data minimization is of utmost importance. It specifies that Article 5 requires jurisdictions to limit personal storage data to a strict minimum.

The GDPR's broad reach means US-based companies handling European residents' personal data must comply with these mandates or risk significant fines and penalties. Several US jurisdictions have also adopted privacy-related regulations that largely follow the EU's lead on data minimization following the GDPR.

For resources that can assist counsel in advising US-based clients on the GDPR, see the GDPR Resources for US Practitioners Toolkit.

US Laws

Counsel for US companies should be aware of the domestic data minimization requirements now (or soon to be) in effect in jurisdictions such as California, Colorado, Connecticut, Delaware, Indiana, Illinois (see below), Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New York (see below), Oregon, Tennessee, Texas, and Virginia, and under the Federal Trade Commission Act (15 U.S.C. §§ 41-58) (FTC Act).

California Consumer Privacy Act

Effective January 1, 2023, the California Privacy Rights Act of 2020 (Cal. Civ. Code §§ 1798.100 to 1798.199.100) (CPRA) amended and supplemented the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199.95; Cal. Code Regs. tit. 11, §§ 7000 to 7102). The CCPA applies to any for-profit entity doing business in California with more than $25 million in gross annual revenue or that conducts major business buying, selling, or sharing consumers' personal information, if they collect or handle California consumers' personal data.

The CCPA as initially adopted (or subsequently amended until 2020) did not contain the principle of data minimization. When amended by the CPRA, the CCPA contained the first explicit data minimization requirement of any US privacy law. Specifically, the CCPA:

- Requires that a company disclose to consumers what personal data it collects, for what purpose, and for how long the company keeps the data.
- Prohibits a company from:
  - collecting additional categories of personal information;
  - using the information it collects beyond its disclosed purpose; and
  - retaining a consumer's personal or sensitive personal information for longer than reasonably necessary beyond the disclosed collection purpose.

  (Cal. Civ. Code Section 1798.100(a)(1)-(3).)
- Mandates that collecting, using, retaining, or sharing personal information must be "reasonably necessary and proportionate" to achieve the business purpose for which the company collected or processed the information (Cal. Civ. Code Section 1798.100(c)).

Similarly, the regulations promulgated by the California Privacy Protection Agency (CPPA) emphasize that a business's "collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve (1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b); or (2) Another disclosed purpose that is compatible with the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c)." (Cal. Code. Regs. §7002(a).)

On April 2, 2024, the CPPA issued Enforcement Advisory No. 2024-01 to provide guidance on the applicability of data minimization to data subject access requests under the CCPA. The Advisory identifies data minimization as "a foundational principle in the CCPA" and states that "Businesses should apply the principle of data minimization to every purpose for which they collect, use, retain, and share consumers' personal information."

For more information about California privacy laws, see the California Privacy Toolkit (CCPA and CPRA).

New York Stop Hacks and Improve Electronic and Security (SHIELD) Act

The New York Stop Hacks and Improve Electronic and Security (SHIELD) Act applies to companies

that own or license New York residents' private information. The SHIELD Act requires companies to apply and maintain reasonable safeguards to protect the private information's security, confidentiality, and integrity, including its data disposal (N.Y. Gen. Bus. Law § 899-bb(2)).

For example, companies can comply with the SHIELD Act by implementing a data security program with certain defined features, including disposing of private information within a reasonable time after the company no longer needs it for business purposes (N.Y. Gen. Bus. Law § 899-bb(2)(b)(ii)(C)(4)).

For more information about the SHIELD Act, see Legal Update, New York Amends Data Breach Notification, Information Security, and Identity Theft Prevention Obligations.

Illinois Biometric Information Privacy Act (BIPA)

The Illinois Biometric Information Privacy Act (BIPA) (740 Ill. Comp. Stat. 14/ to 14/99) relates to biometric information and identifiers, such as facial geometry, iris scans, voice prints, and fingerprints. BIPA applies to private entities that possess biometric identifiers or information. It requires these entities to develop a written, publicly available policy that sets:

- A retention schedule for biometric identifiers or information.
- Guidelines for permanently destroying an individual's identifiers or information at the earlier of:
  - after the entity satisfies its initial purpose for collecting the identifiers or information; or
  - within three years of the last interaction between the individual and the entity.

As a parade of class action lawsuits have shown, an organization's failure to comply with BIPA's mandates can result in steep statutory penalties and fee awards (see, for example, *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535 (N.D. Cal. 2018)). The penalties were so devastatingly steep and potentially annihilative that the Illinois General Assembly amended BIPA to limit damages and provide for electronic consent (IL SB 2979, effective Aug. 2, 2024).

For more information about the BIPA, see Practice Note, BIPA Compliance and Litigation Overview.

Furthermore, as the result of an enforcement action instead of private litigation, Texas Attorney General Ken Paxton in 2024 secured a $1.4 billion settlement with Meta (formerly known as Facebook) to stop the company's practice of capturing and using the personal biometric data of millions of Texans without the authorization required by law (Agreed Final Judgment, *Texas v. Meta Platforms, Inc.*, July 30, 2024).

Federal Trade Commission Act

The FTC Act applies to "all persons engaged in commerce." It prohibits engaging in "unfair methods of competition" and "unfair or deceptive acts or practices in or affecting commerce." (15 U.S.C. § 45(a)(1).) Although the FTC Act may not sound like a data minimization mandate, the FTC has considered unreasonable data security practices to qualify as an unfair or deceptive practice, including collecting consumer data and retaining it longer than a legitimate business purpose justifies (FTC 2023 Privacy and Data Security Update at 12; also see Penalties for Over-Retention Are Becoming More Prevalent).

The FTC also updated its Safeguards Rule that applies to financial institutions effective as of December 1, 2022, and generally requires financial institutions to implement procedures to securely dispose of customer information within two years of it last using that information. However, financial institutions may keep the information longer for a legitimate business or legal purpose. (16 C.F.R. § 314.4(c)(6)(i).)

For more information on:

- The FTC's update to its Safeguards Rule, see Legal Update, FTC Amends Safeguards Rule to Strengthen Data Security Obligations.
- State laws that require businesses and other entities to securely destroy or dispose of personal information they store electronically or physically (or both), see Practice Note, State Data Disposal Laws Chart: Overview.

Other Consumer Privacy Laws

To date, 19 US states have adopted comprehensive data privacy laws that are either now in effect or will be effective by January 1, 2026. Each state's legislation similarly applies to different types of entities and promotes data minimization. Most state privacy laws provide that a covered organization must collect only adequate and relevant personal data limited to what it reasonably needs in relation to the specific purpose for which it processes the data. Only

Rhode Island and Utah's privacy laws do not include requirements for data minimization or a purpose limitation.

For more information about the consumer privacy legislation in these states, see these Legal Updates:

- California Enacts CCPA and CPRA Amendments and Other Privacy-Related Legislation;
- Colorado Attorney General Releases Guidance on Data Security Practices and the Colorado Privacy Act;
- Connecticut Enacts Consumer Privacy Act;
- Kentucky Enacts Consumer Data Privacy Law;
- Minnesota Enacts Consumer Data Privacy Act;
- New Jersey Enacts Consumer Data Privacy Law;
- Oregon Enacts Consumer Privacy Act;
- Utah Enacts Consumer Privacy Act; and
- Virginia Amends Virginia Consumer Data Protection Act.

Also see the Quick Comparison Chart (CPRA and VCDPA) and the Quick Comparison Chart (GDPR and VCDPA).

Penalties for Over-Retention of Personal Data Are Increasingly Prevalent

Due to various legislative and regulatory mandates, organizations that fail to practice proper data hygiene, collect too much consumer data, or over-retain this data risk drawing enforcement actions and potentially hefty penalties. Regulators have demonstrated a heightened willingness to enforce these data minimization mandates. Several developments that illustrate the trend include the following:

- In January 2022, the New York Attorney General reached a settlement with vision benefits provider EyeMed following an investigation into a data security incident. The action concerned a 2020 data breach where hackers accessed an EyeMed email account and exposed the personal information of more than two million consumers. The email account contained content from a six-year period that contained patients' sensitive personal and health information. The Attorney General relied on the SHIELD Act's data minimization mandate to allege it was unreasonable for EyeMed to retain personal information in an email account for up to six years instead of copying it to a more secure location or deleting older messages. The settlement required EyeMed to take on onerous prospective obligations (for example, maintaining a penetration testing program and offering certain customers free daily credit monitoring for two years) and pay a $600,000 penalty. (See Assurance of Discontinuance, *In the Matter of Investigation by Letitia James, Attorney General of the State of New York, of EyeMed Vision Care, LLC*, Assurance No. 21-071 (Jan. 18, 2022).)
- In February 2022, the FTC brought a complaint in California federal district court against two companies related to the company formerly known as Weight Watchers (Kurbo Inc. and WW International) (Legal Update, FTC Announces Settlement with WW International and Kurbo for COPPA Violations). The companies collected personal information from consumers, including minors, using their application (app) for weight management services. The FTC alleged violations of the Children's Online Privacy Protection Act (COPPA) based on the companies' failure to obtain parental consent when they gathered the minors' personal information. The FTC also labeled the companies' over-retention of the minors' personal data for an indefinite period or up to three years as an unfair trade practice under the FTC Act and COPPA. The settlement required the companies to delete the minors' personal information and pay a $1.5 million penalty. (See FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (F.T.C. News Release, March 4, 2022).)
- In June 2022, the FTC finalized an order in its enforcement action against CafePress, an online custom merchandise platform, related to a data breach. Among other data security practices the FTC alleged were deficient, the agency claimed that CafePress put personal information at unnecessary risk because it indefinitely stored the information in the absence of a business need. The FTC considered the platform's indefinite data retention to render its assurances about data security to be false and misleading. It also identified the platform's failure to minimize data as an unfair or deceptive practice under the FTC Act. The settlement required CafePress to adopt stronger data security measures and pay a $500,000 penalty. (See FTC Finalizes Action Against CafePress for Covering Up Data Breach, Lax Security (F.T.C. News Release, June 24, 2022)).

- In May 2024, the FTC finalized a settlement with digital marketing and data aggregator InMarket Media over allegations the company unlawfully collected and used consumers' location data for advertising and marketing. Among other things, the FTC alleged that InMarket "retain[ed] consumer data longer than reasonably necessary for its business purposes leading to likely consumer injury." Under the order, among other things, the company will be required to delete or destroy all the location data it previously collected, and any products produced from this data unless it obtains consumer consent or ensures the data has been deidentified. (FTC Finalizes Order with InMarket Prohibiting It from Selling or Sharing Precise Location Data (F.T.C. News Release, May 1, 2024)).

This trend is almost certain to continue and is likely to pick up steam. Although Congress is no longer considering the proposed federal American Data Privacy and Protection Act (H.R. 8152), section 101 of the discussion draft of the bill would have imposed an express duty of data minimization for certain organizations. In this regard, the ADPPA featured a strong data minimization requirement that entities only collect, use, and transfer data that is reasonably necessary, proportionate, and limited to provide a specific product or service requested by the individual, or a communication reasonably anticipated within the context of the relationship, with some enumerated exceptions.

In April 2024, the federal American Privacy Rights Act of 2024 (H.R. 8188) (APRA) was introduced, which contains similar requirements to the ADPPA. As proposed, APRA-covered entities and service providers are prohibited from collecting, processing, retaining, or transferring personal data beyond what is necessary, proportionate, and limited to provide the requested product or service (or for certain enumerated permissible purposes). In June 2024, APRA was referred to the House Committee on Energy and Commerce for discussion. (Federal Privacy-Related Legislation Tracker: Omnibus Privacy or Data Protection Bills.)

Invest in Proper Data Hygiene Practices Now

Data minimization is no longer an aspirational feature of an organization's approach to privacy. Similarly, data security is not something an organization does only to reduce exposure from a potential data breach. Data minimization and security have become an independent obligation that organizations ignore at their own peril. Now, more than ever, is the time for organizations to carefully evaluate the records they retain and for what purpose. They should develop and document processes to ensure data, especially personal and sensitive data, is disposed of once it no longer serves a business need.

To achieve a healthy information lifestyle, organizations should:

- Revisit and re-evaluate their records retention policies and procedures.
- Update data maps.
- Assess the maturity of their overall information governance systems and programs.

It is also critical that changing practices affecting the retention of personal data are not misaligned with written policies and procedures. The only thing worse than not having a robust information governance program is having a set of policies and procedures that the organization does not follow due to confusion or inconsistency.

Two key components of a svelte information profile are to:

- Mindfully tackle data lakes (meaning, centralized repositories for data storage at scale) and offsite records storage facilities.
- Develop strategies for the defensible disposition of ROT.

The recent legal and regulatory pressures should act as a powerful catalyst for change and provide the motivation necessary to overcome the decision paralysis that organizations often face when challenged to mindfully pursue defensible disposition.

For more resources to help with data hygiene, see the Privacy Compliance and Policies Toolkit.