PRACTICAL LAW
THE JOURNAL

Data Minimization to Avoid Over-Retention of Personal Information

To mitigate the risks of significant costs and penalties, organizations must adhere to data minimization mandates and defensibly dispose of digital debris, including personally identifiable information and digital records that no longer serve a business purpose or otherwise have utility.

MARTIN T. TULLY
PARTNER
REDGRAVE LLP

Martin has over three decades of experience representing clients in complex and high-stakes commercial litigation. He has extensive knowledge concerning e-discovery, information governance, and data privacy and cybersecurity. He counsels clients on best practices for efficient and effective legal, technology, and business solutions. Martin was a drafting team member for The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production.

NICK B. SNAVELY
PARTNER
REDGRAVE LLP

Nick skillfully guides clients through each step of their complex discovery process, including negotiating with opposing and third parties, preparing for and conducting depositions, and working closely with consulting and testifying experts. His extensive discovery experience spans all stages of litigation, including non-dispositive motions, motions for summary judgment, dismissal, and class certification, and mediation.

Reprinted from Practical Law The Journal with permission of Thomson Reuters

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 that their organizational clients are needlessly storing and devise ways to responsibly dispose of it.

In particular, counsel should:

- Create an inventory of the various types of data the organization is storing and derive from that inventory what it is unnecessarily storing.
- Establish a system for defensibly disposing of data that the organization no longer reasonably needs.
- Implement a process for reducing the amount of digital debris retained in the future and periodically update 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) organizations retain personal information.

(For resources to help counsel manage an organization's records and other data, see Records Management Toolkit and Global Records Retention Toolkit on Practical Law; for a model records retention and destruction policy for a non-profit organization, with explanatory notes and drafting tips, see Records Retention and Destruction Policy (Non-Profits) on Practical Law.)

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.

The likelihood that an organization will access aging data decreases exponentially over time, and most data reaches a point after which it no longer has business value. The data eventually becomes digital debris, which industry experts commonly refer to as data that is redundant, obsolete, or trivial (ROT).

Because organizations often retain data by default regardless of its business value, digital debris tends to accumulate indefinitely absent an organization'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 this trend reverses, the trajectory of growing data volumes is unlikely to subside. Therefore, organizations deciding whether to retain data should consider if they currently extract value from it or can potentially do so in the future.

(For more on the costs of data over-retention, see Act Now or Pay Later: The Case for Defensible Disposition of Data on Practical Law.)

REGULATORY RESTRICTIONS

Beyond the monetary costs involved, the unnecessary retention of personally identifiable information, protected health information, payment card industry data, and a host of other sensitive consumer, employee, and business information exposes organizations to potential criminal, civil, and regulatory penalties. Until recently, most legislative and regulatory activity focused on established record-keeping requirements for organizations, such as for tax purposes. However, regulators currently also focus on the rapidly evolving requirements regarding:

- 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 data.

Consequently, storing data that lacks value may perpetuate latent liabilities that escalate over time.

Spearheaded by recent data privacy and cybersecurity mandates, organizations are increasingly restricted to:

- Collecting only the personal data that they absolutely need.
- Using that 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 *Data Minimization Mandates* below.)

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

THE RISE OF DEFENSIBLE DISPOSITION

The US Supreme Court recognized that information governance is an important 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 document retention policies serve important and legitimate business purposes (see, for example, *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 F. App'x 195, 208 (5th Cir. 2007)); *Spanish Peaks Lodge, LLC v. Keybank Nat'l Ass'n*, 2012 WL 895465, at *1 n.3 (W.D. Pa. Mar. 15, 2012) (denying a 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")). (For more on document retention policies, see Drafting a Document Retention Policy on Practical Law.)

The primary purpose of an information governance program, including implementation of a document retention policy, 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 organization'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 involves balancing expected value against expected cost or risk to determine whether a task is sufficiently net positive to warrant proceeding. Decisions on data retention and disposition are no different. An organization's information has value, incurs costs, and can either create or mitigate risks.

REASONABLE RETENTION

Counsel should approach data retention and disposition decisions sensibly. Regulators measure an organization's conduct by considering whether it is reasonable, that is, by evaluating what a typical organization acting with regular prudence under similar circumstances would do. Regulators do not expect or require perfection because this is impossible. An organization's proposed initiatives to dispose of large volumes of ROT data may be impeded by concerns that the data may contain documents relevant to a future legal or regulatory proceeding.

Regardless of whether an organization can identify documents as 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 data. Instead, the regulator

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. Although it is neither practical nor possible for an organization to identify and purge all ROT data, organizations can make significant gains using tactical initiatives that target particular data stores. For example, an organization can significantly reduce hard and soft costs simply by:

- Adopting a framework for classifying the information it creates and receives.
- Remediating the organization's most readily identifiable and addressable ROT data.
- Assigning conservative retention periods to the remainder of the organization's existing data to remediate less readily identifiable ROT data over time.

BIFURCATE INFORMATION

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

Bifurcating information and implementing the necessary policies, procedures, and technologies for the retention and disposition of information helps an organization 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.

DATA MINIMIZATION MANDATES

Defensible disposition and data minimization practices are increasingly necessary for many organizations, especially regarding personal and sensitive data. In recent years, jurisdictions within and outside the US have adopted regulations mandating data minimization related to privacy and consumers' personal information. While the details vary among jurisdictions, several jurisdictions have adopted mandates that essentially prohibit organizations from:

- Collecting more personal data than necessary to fulfill a legitimate purpose.
- Retaining collected data longer than necessary to serve that purpose.

GENERAL DATA PROTECTION REGULATION (GDPR)

As with many aspects of privacy regulation, the EU's GDPR led the way in data minimization (for more information, see Overview of EU General Data Protection Regulation on Practical Law). Article 5 of the GDPR lists six principles for how to process personal data, two of which directly address data minimization. In particular, personal data must be:

- Limited to what is necessary for the purpose of processing the personal data.
- Retained in a way that allows data subject identification for no longer than necessary to process the personal data. (GDPR Article 5(1)(c), (e).)

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

The GDPR's broad reach means that US-based organizations handling EU 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 as set out in the GDPR.

(For resources to assist counsel in advising US-based clients on the GDPR, see GDPR Resources for US Practitioners Toolkit on Practical Law.)

US LAWS

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

(For more on state laws that require organizations to securely destroy or dispose of paper and electronic records containing personal information, see State Data Disposal Laws Chart: Overview on Practical Law.)

California Consumer Privacy Act of 2018 (CCPA)

The CCPA, as amended and supplemented by the California Privacy Rights Act of 2020 (CPRA) (Cal. Civ. Code §§ 1798.100 to 1798.199.100; Cal. Code Regs. tit. 11 §§ 7000-7304) (collectively, 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 did not contain the principle of data minimization. However, as amended, the CCPA is the first US privacy law to contain an explicit data minimization requirement. Specifically, the CCPA:

- Requires that an organization disclose to consumers what personal data it collects, for what purpose it collects the data, and for how long it keeps the data.
- Prohibits an organization from:
  - collecting additional categories of personal information that it did not disclose;
  - 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 § 1798.100(a)(1)-(3).)
- Mandates that the collection, use, retention, or sharing of personal information must be "reasonably necessary and proportionate" to achieve the business purpose for which the organization collected or processed the information (Cal. Civ. Code § 1798.100(c)).

(For guidance on drafting a CCPA/CPRA privacy policy that provides specific disclosures about an organization's information protection practices, see Drafting a CCPA/CPRA Privacy Policy in the September 2023 issue of *Practical Law The Journal*.)

Similarly, the regulations promulgated by the California Privacy Protection Agency (CPPA) emphasize that an organization's "collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate" to achieve:

- The purpose for which the personal information was collected or processed, which must comply with the requirements set forth in subsection (b).
- Another disclosed purpose that is compatible with the context in which the personal information was collected, which must comply with the requirements set forth in subsection (c). (Cal. Code Regs. tit. § 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 organizations "should apply this principle [of data minimization] to every purpose for which they collect, use, retain, and share consumers' personal information" (CPPA: Enforcement Advisory No. 2024-01).

(For resources to help counsel understand California's various privacy law requirements, including the CCPA and CPRA, see California Privacy Toolkit (CCPA and CPRA) on Practical Law.)

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

The SHIELD Act applies to organizations that own or license New York residents' private information. It requires organizations to apply and maintain reasonable safeguards to protect the private information's security, confidentiality, and integrity, including its disposal (N.Y. Gen. Bus. Law § 899-bb(2)). For example, an organization 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 organization no longer needs it for business purposes (N.Y. Gen. Bus. Law § 899-bb(2)(b)(ii)(C)(4)).

(For more on the SHIELD Act, see New York Amends Data Breach Notification, Information Security, and Identity Theft Prevention Obligations on Practical Law.)

Illinois and Texas Biometrics Laws

The Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14/1 to 14/99) applies to private entities that possess biometric identifiers or information, such as facial geometry, iris scans, voiceprints, and fingerprints. 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 the following:
  - 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 entity.

As shown by the filing of several class action lawsuits, an organization that fails to comply with BIPA's mandates may face steep statutory penalties and fee awards (see, for example, Order re: Final Approval, Attorneys' Fees and Costs, and Incentive Awards, *In re Facebook Biometric Info. Privacy Litig.*, No. 15-3747 (N.D. Cal. Feb. 26, 2021) (Docket Nos. 499, 517) (approving a $650 million settlement)). Indeed, the penalties in BIPA cases were so devastatingly steep and potentially annihilative that the Illinois General Assembly amended BIPA to limit damages and clarify that organizations may obtain written consent electronically (IL SB 2979 (effective Aug. 2, 2024); for more information, see Illinois Amends BIPA to Limit Statutory Damages on Practical Law; for more on BIPA generally, see BIPA Compliance and Litigation in the August 2023 issue of *Practical Law The Journal*).

Additionally, in a 2024 enforcement action under the Texas Capture or Use of Biometric Identifier Act (TX Bus & Com § 503.001) and Data Privacy and Security Act (TX Bus & Com §§ 541.001 to 541.205), Texas Attorney General Ken Paxton secured a $1.4 billion settlement with Meta (formerly known as Facebook). This settlement aimed to stop the organization's practice of capturing and using the personal biometric data of millions of Texans without legal authorization. (Agreed Final Judgment, Texas v. Meta Platforms, Inc. (July 30, 2024).)

FTC Act

The FTC Act prohibits all persons engaged in commerce from using "[u]nfair 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 Federal Trade Commission (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: The Federal Trade Commission 2023 Privacy and Data Security Update at 12).

The FTC also updated its Safeguards Rule that applies to financial institutions, which became effective on December 1, 2022. The Safeguards Rule generally requires financial institutions to implement procedures to securely dispose of customer information within two years of its last use of 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, see FTC Amends Safeguards Rule to Strengthen Data Security Obligations on Practical Law.)

Other Consumer Privacy Laws

To date, 19 US states have adopted comprehensive data privacy laws that are currently in effect or will be in effect by January 1, 2026. Each state's legislation similarly applies to different types of organizations and promotes data minimization. Most state privacy laws require covered organizations to collect only adequate and relevant personal data that is limited to what the organization reasonably needs in relation to the specific purpose for which it processes the data. Only Rhode Island's and Utah's privacy laws do not include requirements for data minimization or a purpose limitation.

(For more on consumer privacy legislation in select states, see Colorado Attorney General Releases Guidance on Data Security Practices and the Colorado Privacy Act, New Jersey Enacts Consumer Data Privacy Law, Comparing the CCPA and VCDPA: Overview, and Comparing the GDPR and VCDPA: Overview on Practical Law.)

PENALTIES FOR OVER-RETENTION OF PERSONAL DATA

Due to various legislative and regulatory mandates, organizations risk enforcement actions and potentially hefty penalties if they:

- Fail to practice proper data hygiene.
- Collect excessive consumer data.
- Retain data longer than necessary.

Regulators have demonstrated a heightened willingness to enforce data minimization mandates. Developments that illustrate this 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 had accessed an EyeMed email account and exposed the personal information of more than two million consumers. The compromised email account contained patients' sensitive personal and health information from a six-year period. The Attorney General relied on the SHIELD Act's data minimization mandate to allege that 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 the older messages. The settlement required EyeMed to implement onerous prospective obligations (such as 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 a California federal district court against two companies related to the company formerly known as Weight Watchers (Kurbo Inc. and WW International) (for more information, see FTC Announces Settlement with WW International and Kurbo for COPPA Violations on Practical Law). The companies had collected personal information from consumers, including minors, using their application 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 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 Press Release: FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2022); for more on COPPA, see COPPA Compliance in the June 2024 issue of *Practical Law The Journal*.)
- In June 2022, the FTC finalized an order in its enforcement action against CafePress, an online custom merchandise platform, related to a data breach. The FTC alleged deficient data security practices, including that CafePress had unnecessarily retained personal information by indefinitely storing it without a business need. The FTC determined that CafePress's practice of indefinite data retention contradicted its assurances about data security, rendering these assurances 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 News Release: FTC Finalizes Action Against CafePress for Covering Up Data Breach, Lax Security (June 24, 2022).)

- In May 2024, the FTC finalized a settlement with digital marketing and data aggregator InMarket Media over allegations that the company had unlawfully collected and used consumers' location data for advertising and marketing. The FTC's allegations included that InMarket had "retain[ed] consumer data longer than reasonably necessary for its business purposes leading to likely consumer injury" (Complaint, In the Matter of InMarket Media, LLC, at 6 (2023)). Among other provisions, the FTC order requires the company to delete or destroy all previously collected location data and any products produced from this data, unless it obtains consumer consent or ensures the data has been deidentified. (See FTC News Release: FTC Finalizes Order with InMarket Prohibiting It from Selling or Sharing Precise Location Data (May 1, 2024).)

This trend is almost certain to continue and is likely to accelerate. Although Congress is no longer considering the proposed federal American Data Privacy and Protection Act (ADPPA) (H.R. 8152), Section 101 of the discussion draft of the bill would have expressly imposed a strong duty of data minimization on certain organizations. The ADPPA would have required 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 that falls under certain permissible purposes, such as to deliver a communication that is reasonably anticipated within the context of the relationship.

In April 2024, the federal American Privacy Rights Act of 2024 (APRA) (H.R. 8188) 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 either providing the requested product or service or fulfilling certain enumerated permissible purposes. In June 2024, APRA was referred to the House Committee on Energy and Commerce for discussion. (See H.R. 8818 — American Privacy Rights Act of 2024.)

DATA HYGIENE BEST PRACTICES

Data minimization is no longer an aspirational feature of an organization's approach to privacy. Similarly, data security goes beyond merely reducing exposure to a potential data breach. Data minimization and security have become independent legal obligations that organizations ignore at their own peril. Now more than ever, organizations must 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 document retention policies and procedures.
- Update data maps, which describe what data resides where within an organization and how data flows within and among its various internal and external information systems.
- Assess the maturity of their overall information governance systems and programs.
- Ensure that changing practices affecting the retention of personal data are not misaligned with written policies and procedures. While the absence of a robust information governance program is problematic, having a set of policies and procedures that the organization does not follow due to confusion or inconsistency will also lead to issues.

Two key components of a streamlined information profile are to:

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

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

(For resources to assist counsel in creating, implementing, and reviewing US privacy compliance and information management programs, see Privacy Compliance and Policies Toolkit on Practical Law.)