Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Compliance Imperatives For Defensible Data Disposal

By **Julia Brickell** (July 26, 2019, 4:43 PM EDT)

Julia Brickell

A $5 billion Federal Trade Commission compliance fine for Facebook Inc.[1] A £183 million UK compliance fine for British Airways. Marriott International faces a £99.2 million fine for data breach.[2] The hits just keep coming. Escalating data breach costs. Spiraling e-discovery costs. Defensible disposal of corporate data presents an excellent opportunity to mitigate the impact of these data-driven risks. Indeed, its time has finally come.

For years, even before the advent of corporate email, managing data to retain what is needed and delete the remainder has been back-burnered in many organizations. A cleanup endeavor lacking in allure, the chief financial officer’s reluctance to spend has easily overridden the tepid enthusiasm of the business to manage information stores.

More recently, the call of big data — with promise of data-mined business intelligence — coupled with the notion that data storage is cheap, has derailed data management efforts even further. Meanwhile, corporate data sources multiply, and volume just keeps growing.

It is now clear that the “storage is cheap” mindset carries consequences. The sheer size and multiplicity of data types expose companies to increasing costs and risk. Data locations and their regulated content need to be mapped and managed. Vendors and their infrastructures need to be assessed. Access controls need to be designed and maintained.

Security methods need to be analyzed and managed for every application and associated storage location — both inside and outside the company. Retaining unneeded data has an impact on litigation expense as well, with more data in play for discovery generating greater costs.

Growing Threats: Data Breach and Expanding Regulatory Risks

Every organization is at risk of data breach, public or private, no matter the industry vertical — targeted by organized criminal groups, nation-state or state-affiliated entities and internal actors with motives ranging from financial gain to espionage.

Verizon Wireless’s 2019 data breach investigations report, which rigorously examined an acknowledged “sample” of data incidents, captured 41,686 security incidents, of which 2,013 were confirmed data breaches (an incident resulting in confirmed disclosure to an unauthorized party).

Even well-secured environments may be at risk; an estimated 21% of breaches are attributable to employee errors.[3] And, since the General Data Protection Regulation went into effect a little over a year ago, European data protection authorities confirm that almost 90,000 separate data breach notifications have been received from organizations attempting to comply with the GDPR, along with nearly 145,000 complaints and inquiries reported by concerned citizens.[4]

In all cases, data is the prize. Disposing of that which is unnecessary can play an important role in keeping damage to a minimum.

Regulations (and interpretations) governing retained data have expanded as well, creating risk beyond breach for companies that hold on to data they no longer need. GDPR and the Payment Card Industry Data Security Standard impose requirements that companies maintain protected data no longer than necessary.

The Health Insurance Portability and Accountability Act mandates that regulated entities require vendors to sign business associate agreements that promise data disposal. The FTC may consider overdisclosure or underprotection of private information an unfair trade practice.

Fines for compliance missteps? A taxi company in Denmark received a fine of over $150,000 (1.2 million kroner) just for keeping personal contact information longer than necessary.[5] Google LLC was fined €50 million for collecting and using personal data without adequate explanation of how it would be used for advertising.[6] A Portuguese hospital was fined €400,000 for allowing more than the necessary staff to access patient records.[7] Resource costs and reputational harm just pile on the damage.

Data Disposal: New Return on Investment, a Refreshed Imperative

Companies that factor in the true costs and risks associated with their vast data stores are doing themselves a service. A fresh look at data disposal is warranted. Indeed, the ROI for disposing of data has shifted, making data disposal arguments more compelling:

- Daily data breaches increase the projected cost of keeping unnecessary data.

- Regulations increasingly call for private data to be retained for no longer than it is needed.

- Electronic discovery costs have not gone away, and courts have little sympathy for data hoarders; keeping only what is needed reduces preservation, collection and processing and review costs should an e-discovery need arise.

- Advanced methods, such as targeted search and analytics, make disposal efforts easier, reducing costs and business interruption.

Computing the ROI may not be necessary if regulations mandate that a company dispose of data regardless, but if needed in order to acquire a commitment from senior management, it is worth the effort. It would be natural in this age of regulated data for the compliance or information governance function to take charge. The logical data protection allies are information technology and information security, although those functions lack ownership of content, the motivating force.

Where to begin?

A good place to start is the C-suite. Data disposal will take a thoughtful, organized and prioritized effort with strong central leadership to maintain focus. This effort requires ongoing input from a number of sources, so the next step is to build a cross-functional team. The team should include — along with compliance and information governance — IT, legal, and representatives of individual business units.

Steps to Take

Overall, the company needs to know what data it has, what it needs to keep, and what it can dispose of. This takes time and a concerted effort, to be sure, but isn’t inherently difficult.

Step 1

Prepare an inventory. Drive an effort to undertake an honest assessment of data realities in the company and take inventory. Interview IT and business units. What systems exist and how is data being managed now? Are there legacy systems with stockpiles of old data? Stray media? Are there data stores in official cloud applications? What about in applications certain departments or enterprising business folk have used on the side?

Document the results.

Step 2

Confirm and define retention needs. Make sure retention imperatives for business, regulatory or legal purposes are well-defined. Legal holds can usually be analyzed, then updated or released as warranted by an in-house team. (Note that data that has been collected for legal reasons has often been copied and is thus duplicative. When the hold is lifted, such data may be able to be deleted altogether.)

Step 3

Prioritize data sources. With the cross-functional team, analyze the inventory. Consider each source and the nature of the data it contains. Ask the business for insight, and use common sense. How likely is it that a particular source contains data that must be retained? If likely, is the data duplicative of another source? Can the data to be retained be identified and separated at a high level (by date, custodian, or folder, for example) from unnecessary data? If not, the work is more complex and may require use of the type of tools described below. Not sure? Sample the data. A statistically sound sampling process will help ensure a defensible action.

When prioritizing, strike a balance between going after easy wins — which reduce current costs and create momentum — and highest risks. Consider tackling easy projects first (duplicative data sources or email of departed employees, for example) while taking time to plan for more valuable or precarious data stores — the ones that bring the highest ROI.

Step 4

Evaluate tools. As you plan, consider available categorization tools that can help identify and segregate data. The right tools, properly used, can achieve excellent results with truly defensible levels of accuracy. As they have different strengths and weaknesses, assess them in light of particular workflows, data characteristics and retention needs.

Step 5

Clarify secure disposal. Articulate clear rules for secure disposal. The National Institute of Standards and Technology and other frameworks provide insight, and it is advisable to have clear rules so that unneeded regulated and sensitive business information in all formats and applications is disposed of safely.

As the security team (and regulators) know, dumpster diving, reading memory chips from disposed copier machines and reconstructing fragments of deleted information can be on the path to an avoidable data breach or litigation expense.

Step 6

Implement. Don’t stop now! Methodically address the data stores as they have been prioritized using the selected tools and methods to identify and securely dispose of unneeded data. Be mindful of necessary expertise; to be defensible, analytics tools and classification methodologies must be properly calibrated and deployed.

Remember that any progress is motivating. And — this is important — document the determinations that are made, and let decisions about how to handle existing data inform data management going forward.

Bottom Line

The ROI for defensible data deletion has turned to positive, at least for companies that are at risk of regulatory fines or data breach — which is pretty much everyone. With team energy behind the effort and armed with the right tools and expertise, data disposal can be planned, managed and defended. Those in the C-suite will be able to rest easier once a concerted effort is underway. Although there is no quick fix, the expertise exists to support the imperative. Procrastination is risky — get started!

Julia Brickell is executive managing director and general counsel of H5.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html

[2] https://www.natlawreview.com/article/uk-ico-proposes-gdpr-fines-british-airways-and-marriott-data-breaches

[3] https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/

[4] https://www.techrepublic.com/article/gdpr-fines-levied-so-far-the-lessons-businesses-can-learn/
[5] https://www.compliancejunction.com/danish-dpa-issues-first-ever-gdpr-fine-against-taxi-company/

[6] https://www.compliancejunction.com/french-data-protection-agency-google-gdpr-penalty/

[7] https://www.law.com/corpcounsel/2018/11/09/gdpr-fine-against-portuguese-hospital-puts-health-care-providers-on-alert/