**Global Data Privacy and Security Team**

# Document Retention and Collection Policies At A Glance

Data minimization can be a powerful – and seemingly simple – data security measure. The term refers to retaining the least amount of personal information that is necessary in order for an organization to function. Less information means that there is less that the organization needs to protect, and less opportunity for information to be lost or stolen.

In practice data minimization requires organizations to fully understand where they collect information, why they collect information, and where it is stored. It also requires difficult decisions regarding what information the organization will likely need in the future from a business perspective, and what impact having limited consumer or employee records may have on potential legal disputes if they arise. For example, an organization that chooses to implement a 30 day or 60 day automatic "roll off" policy for employees' may not be able to identify email exchanges between an employee and a vendor that relate to a contract dispute which arises months later.

| Average size of employee inbox.* | Number of pages of Excel data files that could be on a 100GB hard drive.† | Length of time identifying search history is kept by major search engines. |
|---|---|---|
| 8,000 | 16 MILLION | 9 MONTHS‡ – 18 MONTHS§ |

**"The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and hold onto personal information unnecessary to an identified purpose. Keeping data on the off-chance that it might prove useful is not consistent with privacy best practices."**

*- Federal Trade Commission Chairwoman Edith Ramirez***

Bryan Cave's Global Data Privacy and Security Team has responded to hundreds of data security breaches and routinely helps clients, before a breach happens, analyze and improve upon their ability to respond to a breach if (or when) one occurs.

For more Information Contact:

**David A. Zetoony**
Partner
david.zetoony@bryancave.com

1155 F Street, N.W.
Washington, D.C. 20004
T: 1 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386
T: 1 303 444 5955

*Dave Troy, "The Truth About Email: What's A Normal Inbox?" (Apr. 5, 2013).
†*See* http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitepapers/adi_fs_pagesinagigabyte.pdf (last viewed Dec. 2014).
‡Google Official Blog, Another Step to Protect User Privacy, Posted Sept. 8, 2008
§Yahoo Data Storage and Anonymization FAQ available at https://info.yahoo.com/privacy/us/yahoo/drfaq (last viewed Dec. 2014).
**The Privacy Challenges of Big Data: A View From the Lifeguard's Chair, Keynote Address Technology Policy Institute Aspen Forum (Aug. 19, 2013).

**What to think about when designing a retention policy:**

| | |
|---|---|
| ✓ | Do you systematically track all of the data fields that your organization collects from consumers and employees? |
| ✓ | Do you systematically apply retention periods to each data field that you collect? |
| ✓ | Do those retention periods reflect the current business needs, or estimates as to possible future business needs? |
| ✓ | For a particular data field, what time period is typical in your industry and for the type of data at issue? |
| ✓ | Should you attempt to anonymize (sometimes called de-identify) data after a certain amount of time? |
| ✓ | If you do anonymize data, is your organization's process of anonymization considered legally sufficient? |
| ✓ | What data and documents are you legally required to retain, and for how long must they be retained? |
| ✓ | If you decide to retain other data and documents how does it increase, or decrease, your legal risk? |
| ✓ | What additional data that, if collected, is your organization likely to need in the next 12 months? |
| ✓ | What steps are taken to irrevocably destroy data that is no longer needed? |