A Forgotten Privacy Concern: Dumpster Diving For Discarded Data

By Howard Fienberg, MRA

At this moment, whether on hard drives you thought you wiped before giving them away, or on paper piled up in the recycling bin, confidential research data is readily available to identity thieves. Despite concerns about high-tech computer network hacking or criminal-minded employees, simple carelessness is the greatest threat to data security – and simple policies and recurring education are the best tools to counter that threat.

Oops

- Last summer, unidentified men were filmed by local TV news cameras removing paperwork from dumpsters behind the San Francisco Human Services Department – paperwork, such as records of personal information like Social Security numbers, ID cards, names and addresses;
- Last spring, schematics labeled for the planned Freedom Tower were found in a New York City public trash bin. The plans, discarded by a contractor, were labeled "Secure Document – Confidential";
- In 2007, CVS became liable for fines and lawsuits after authorities in Texas discovered customer records in the trash behind a store, including active debit and credit card numbers, complete with expiration dates.

"Out of sight, out of mind" is not a tenable or survivable data disposal policy. Personal or client information discarded in the trash or recycling bin is legally and effectively open to anyone. So is any data stored on discarded or donated computer technology, like hard drives and thumb drives, once the devices are thrown away or donated to charity.

The weakest link in the data security chain is the personnel implementing it – or more tragically, disregarding it. What can you do to shore up your data disposal policies?

Legal Requirements for Data Disposal

Though the law does not apply to most conduct of survey and opinion research, any business or individual who uses a consumer report or information derived from one for a business purpose is subject to the Fair Credit Reporting Act (FCRA) "Disposal Rule." The rule requires the proper disposal of information in consumer reports and records to protect against "unauthorized access to or use of the information."

The standard for the proper disposal of data is flexible, and allows researchers to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods and changes in technology.

Data Disposal Best Practices

Although the Disposal Rule applies to consumer reports, and the information derived from them, MRA encourages anyone who disposes of any records containing personal information to take similar protective measures. These measures should be reasonable and appropriate to prevent the unauthorized access to – or use of – such information. Organizations should also exercise due diligence when working with disposal experts and companies.

Reasonable measures could include establishing and complying with policies to:

- burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- conduct due diligence and hire a document destruction contractor to dispose

of material specifically identified as consumer report information consistent with the rule.

Due diligence could include:

- reviewing an independent audit of a disposal company's operations and/or its compliance with the rule;
- obtaining information about the disposal company from several references;
- requiring that the disposal company be certified by a recognized trade association;
- reviewing and evaluating the disposal company's information security policies or procedures.

Other Data Disposal Policies to Consider

- How long should data be stored? Only as long as necessary. Consider establishing a schedule for regular reviews of existing data (electronic and paper) and whether or not it can be disposed.
- Keep a record of what set of data was disposed when and how. In the event of an audit or litigation, this could be required by law.
- Recycling bins are not an appropriate disposal place for personal information. Aside from any number of unknown people having access to that information once it goes in the bin, recycling companies often keep paper and other materials in storage to await use in other products. The recycling companies have no responsibility to your organization or to the people whose data you're exposing. Paper or electronic data should never end up in recycling until after is has been shredded or destroyed.
- Hitting "empty recycle bin" on the Windows desktop is not necessarily a sufficient method for electronic data disposal. See the FTC link below for tips on disposing of electronic equipment that may still contain personal information.
- Who is authorized within your organization to destroy data? Should lower-level employees or contractors, who may not be authorized to handle the information during a research study, be given the responsibility to dispose of it? Should the janitorial staff be entrusted? What kind of upper-management oversight is needed?
- Most importantly, organizations need to educate employees and contractors on your policies and procedures – every person that could handle personal information needs to know what to do with it.

For more information:

- Federal Trade Commission on Computer Disposal: www.onguardonline.gov/topics/computer-disposal.aspx
- National Association for Information Destruction: www.naidonline.org

Disclaimer: The information provided in this article is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. MRA advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

Howard Fienberg is director of Government Affairs at MRA. He can be reached at howard.fienberg@mra-net.org.