This Tape Will Self-Destruct in Five Seconds — Self-Destructing Digital Data

If you remember *Mission Impossible*, you no doubt recall Jim Phelps (played by Peter Graves) receiving his instructions — "Your mission, should you choose to accept it…" — on a tape that self-destructs five seconds after playing. The reel-to-reel tape played on a small recorder, and its disintegration was accompanied by an ominous cloud of smoke. *Dun-dun-da-da, dun-dun-da-da…*

Last week, we went back to the future as several articles surfaced about Vanish, a technology to **automatically render electronic data unrecoverable** at a specified time in the future. Vanish is designed to enhance a user's privacy by creating data that will automatically self-destruct at a specified time in the future, making later recovery of the data essentially *impossible* by the user, by Google, by a hacker that breaks in, or even by someone with a warrant for the data. The data essentially self-destructs and becomes permanently unreadable.

The technology is based on the use of a remote encryption key that is time-based, and never in the user's possession. Instead, the key is maintained in pieces, distributed throughout a peer-to-peer network. In theory, the distribution of the encryption key prevents the reassembly of the data.[1]

The concept is seductive — imagine if you could know that your e-mail messages (or Facebook posts, or backup tapes) were completely safe after the expiration of a pre-determined period of time. For example, you could send an e-mail to a confidant, and have it self-destruct in eight hours. The technology would give a user the confidence of knowing that, unless copied elsewhere, a months-old, or even years-old, e-mail would not reappear beyond the document's "expiration date."[2]

The legal implications of Vanish technology in the business world, where spoliation of evidence (i.e., the willful or negligent destruction of evidence when there is a legal duty to preserve it) are enormous.

In the White Paper promoting Vanish, the authors cite an example of Ann, who e-mails a confidant about her pending divorce. The obvious question that arises in Ann's situation, which is not addressed in the White Paper, is that if the e-mail is potentially relevant and thus discoverable in the pending litigation with her husband, Ann may have a legal duty not to use the Vanish technology because it could be considered spoliation. In other words, it seems that the Vanish technology requires careful evaluation before considering its adoption and/or use in business.

Another consideration, aside from the legal requirement to preserve records reasonably anticipated to relate to pending or anticipated litigation, is that for every embarrassing or sensitive e-mail that may appear in a client's records, there are at least an equal number of e-mails that may help exonerate, excuse or add crucial context for explaining a client's actions. Thus, it is likely not possible to accurately predict, at the time a record is created, the proper lifespan of the

document. Unless the Vanish technology allows for a failsafe override, this technology may present as many risks as benefits to potential users.

For example, consider what happens when a duty to preserve attaches to information that has not yet "Vanished." If nothing is done — as between the duty to preserve and Vanish — Vanish wins. Once the encryption key associated with the electronically stored information (ESI) expires, the ESI is rendered unrecoverable. However, a court could find that the user *should have* preserved the data before it was rendered unrecoverable, and *should have* kept a recoverable copy of the data. A court could well find that, at a *minimum*, the custodian should maintain a screen capture, or at least an image of the screen, preserving (i.e., not spoiling) the evidence.

These risks are aggravated by the vagaries of litigation, when, at the outset, it is often not clear what facts will be relevant. In all cases, it is counsel's obligation to ensure that there are reasonable steps taken to preserve the ESI likely to lead to the discovery of admissible evidence. If Vanish technology is used, it is conceivable that the automatic destruction would run its course long before the relevance of the data is established. In some instances, Vanish technology could render relevant data unusable. It could be argued that if Vanish is in use, either: (i) the keys to destroying the data must be preserved[3] — which, as the technology is described, cannot (or cannot easily) be done; or (ii) any Vanish documents that *will be* relevant to pending or anticipated litigation have to be identified and copied before they expire.

Consider, too, Vanish technology's implications for a broker-dealer subject to SEC Rule 17a-4, which requires, among other things, that the broker-dealer retain for three years originals of all communications received. What should the broker-dealer do about a communication that will expire? To comply with the rule, is the broker-dealer required to immediately make a three-year copy of any Vanish communications? Should the broker-dealer automatically reject all communications that are programmed to self-destruct in less than the required three-year period?

Finally, it is important to note that Vanish does not guarantee that the Vanish message's content has been expunged from all destinations. It may be technologically feasible, and likely rather easy, for the recipient of a Vanish message to retain a decrypted copy of the message in an ordinary version of the data.

The Vanish team has presented an interesting technology in its paper. Concerns exist, however, as to how the technology intersects with the legal obligations to preserve records. While Vanish and similar technologies have many potential uses,[4] practical implications of the technology on clients' business operations are necessary to assess before any business should seriously consider implementing Vanish technology.

———

[1] Indeed, even the key pieces could be stored in an encrypted form and that encrypted information could itself expire using yet-another key.
[2] The 17-page Vanish paper entitled Vanish: Increasing Data Privacy with Self-Destructing Data, authored by Roxana Geambasu, Tadayoshi Kohno, Amit Levy, Henry M. Levy, and presented in Proceedings of the USENIX Security Symposium, Montreal, Canada, August 2009. (http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.pdf) illustrates its utility by using a fictional case involving Ann, a woman who exchanges e-mails with a close friend about problems in her marriage. Ann wants the messages to self-destruct, ensuring that the messages will not become a source of embarrassment. Such control over her own communications is a legitimate concern regardless of the outcome of her marital difficulties. If Ann resolves the difficulties with her husband, the messages could be a source of embarrassment. If the problems are not resolved and Ann becomes involved in a divorce, the messages could be the subject of litigation.
[3] According to the Vanish paper, the encryption keys used by Vanish are never in the user's possession; rather, they are retrieved from a distributed external peer-to- peer file sharing network outside the control of the user. If that is correct, it may be that the keys cannot be preserved, and thus, in practical terms, they may be out of the control of court.
[4] One example would include protecting transitory information that is being only temporarily stored by common carriers for forwarding purposes.

This *GT Alert* was prepared by **Adam Landa** and **Phil Cohen.** Questions about this information can be directed to:

- **Adam Landa —** 212.801.9290 (landaa@gtlaw.com)
- **Phil Cohen —** 212.801.2145 (cohenp@gtlaw.com)
- Or your Greenberg Traurig attorney

Albany
518.689.1400

Amsterdam
+31 20 301 7300

Atlanta
678.553.2100

Austin
512.320.7200

Boston
617.310.6000

Chicago
312.456.8400

Dallas
214.665.3600

Delaware
302.661.7000

Denver
303.572.6500

Fort Lauderdale
954.765.0500

Houston
713.374.3500

Las Vegas
702.792.3773

Los Angeles
310.586.7700

London*
+44 (0)203 349 8700

Miami
305.579.0500

New Jersey
973.360.7900

New York
212.801.9200

Orange County
949.732.6500

Orlando
407.420.1000

Palm Beach County North
561.650.7900

Palm Beach County South
561.955.7600

Philadelphia
215.988.7800

Phoenix
602.445.8000

Sacramento
916.442.1111

Shanghai
+86 21 6391 6633

Silicon Valley
650.328.8500

Tallahassee
850.222.6891

Tampa
813.318.5700

Tysons Corner
703.749.1300

Washington, D.C.
202.331.3100

White Plains
914.286.2900

Zurich
+41 44 224 22 44