Is There Privacy Beyond Death?

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI

Written February, 2005
First Published in the CSI March 2005 Alert

One of my New Year's resolutions was to create a will. Since I have two young children, this seems to be a prudent move (yes, I should have already had one). As I was writing it, contemplating to whom I would give my physical possessions, I read a news report about a family who wanted to obtain the email messages of their son who had been killed in Iraq. Wow; I hadn't thought about all my electronic virtual possessions, such as emails and files. What type of information is contained within my messages and files? What should, or would I want, my survivors be able to view? What would my own multiple mail service providers do with all my messages? I wonder, how many companies have thought of the related issues?

Privacy After Death for Email Accounts

Death ends a life, not a relationship.
--Jack Lemmon

U.S. Lance Cpl. Justin M. Ellsworth was killed in Iraq on November 13, 2004. He had a Yahoo! email account, and after his death his family requested to get access to his messages. However, Yahoo!'s privacy policy does not allow for giving others access to their subscribers' accounts, their terms of service are to erase all accounts that are inactive for 90 days, and users agree in their sign-up contract that their account is non-transferable and will terminate upon death with all contents therein permanently deleted. Yahoo! did not give the family the email messages. This event was widely reported and many discussions subsequently occurred.

Yahoo! made a decision to follow the terms of its service agreement and privacy policy, for which over 40 million of their other account holders have also agreed. Yahoo!'s policy and terms of service clearly states that survivors have no rights to email accounts of the deceased. Yahoo! apparently realized any deviation or exceptions to this could bring them under the scrutiny of the U.S. Federal Trade Commission (FTC). After all, the FTC has cracked down in recent years on a variety of companies, such as Microsoft, DoubleClick, Intel, and several others for infringements of posted privacy policies.

This situation truly does demonstrate the humanity of dealing with information protection, and how important policies and procedures are to address such situations. An important aspect to consider that often gets overlooked is how an exception to existing policies and procedures would potentially impact not only the reputation and memory of the deceased, but also how such disclosure could impact others who are deceased, as well as others still living. What if there were correspondences with other people that the deceased did not want anyone else to know about? Or, that the other correspondents never wanted to share with anyone except for the deceased? And, perhaps people were sending messages to the deceased that were unwanted, but could give the wrong impression to people reading and misinterpreting them. You are then entering territories that involve the privacy of others, still living and possibly deceased.

True, Yahoo! could probably have offered to send the family only those messages that were exchanged specifically with the family members themselves, and not send any others. However, how realistic would it be for a company to do such analysis, invest the time do such sorting, and make such decisions? What would happen if some messages to other non-family members slipped through anyway? What if the non-family member correspondents then wanted access to their message exchanges? And, in doing such sorting, it is likely the Yahoo! representatives would have to read the content of Lance Cpl. Justin M. Ellsworth's email messages. Would he have wanted that? Is it fair to read messages of the deceased without them being able to provide context or explanation for information that may be misinterpreted? Would his surviving family members, friends and acquaintances that exchanged messages with him want that? It is speculative to try and assume the privacy wishes of those who are no longer with us. Would you want someone to represent your privacy decisions after your death? Perhaps, but then again, perhaps not. It certain muddies the privacy waters.

This situation raised many questions about privacy after death, the privacy rights of families of the deceased, the privacy of emails, and the privacy of information stored in other forms. And, how does having access to email messages and other electronic forms of information differ from hard copies of information? Or, with recorded voice communications? Does it differ? Should the representation of information and thoughts within electronic format be considered differently from hard copies of the same messages? So, who really does own your email after you die?

Privacy After Death and Copyrights

Some lawyers have reported their beliefs that emails are copyrighted property just like other possessions, and as property would pass to the deceased executors. But what about the copyright rights of the people who were at the other end of the messages? Don't they still have property rights as well that would allow them to not share the emails? And, is it feasible that email messages, which basically are out of the sender's control once the "send" button is hit, have copyrights and ownership attached anyway? Some lawyers argue the contents of emails remain the property of those who wrote them. When the email service subscribers sign on to an email service and agree to their contractual terms of use, they may have given permission to extinguish such rights according to the mail service provider's terms of service. However, those exchanging messages with the subscriber did not agree to those terms of service, so they would not be bound by such terms, would they? The answer to ownership is not clear-cut.

One solution is to have very clear email, messaging and privacy policies, and give subscribers of email, and other types of messaging services, the option to specifically designate whether they want account information passed on to specific persons in the event of death, or want their email messages completely deleted at such time. This way the deceased has made the decision about preserving their privacy before their death, and takes this decision out of the hands of their surviving family members. Shouldn't privacy about the deceased

really be about what the deceased wanted instead of what other people want following his or her death?

Privacy After Death and the U.S. Freedom of Information Act (FOIA)
Under the U.S. Privacy Act, privacy rights are extinguished at death. However, under the subsequent U.S. FOIA, the privacy interests of a decedent's survivors may be considered under Exemption 6. For example, in March 2004 the Supreme Court decided an FOIA case involving photos of Vince Foster, a Clinton White House aide who committed suicide in 1993. The principal issue was whether his relatives had a protectable privacy interest. Because Foster is deceased his privacy interest, generally under the FOIA, was not at stake. In Foster's case, the court held that the FOIA protected the surviving family members' right to personal privacy with respect to images of a close relative's death scene.

The FOIA survivor privacy protection principle was reportedly first applied by the U.S. government to the Department of Justice records for the investigation into the assassination of Dr. Martin Luther King, Jr., in the case of Lesar v. United States Department of Justice in 1978. In essence the survivor privacy principle is based upon protecting survivors in cases of extraordinary sensitivity from "disruption [to] their peace of mind." Subsequent cases, such as ones involving President John F. Kennedy, Vince Foster, and the tragic deaths of the astronauts in the Space Shuttle Challenger, have cited this seminal case, speaking of the surviving family members' "own peace of mind and tranquility". With electronic communications, should people outside of family members who exchanged emails, instant messages, voices mails, and other such communications with the deceased also be considered as survivors? The law is not clear on this consideration of our evolving new technology frontier from what I could find. Because of this it behooves companies to think about what they will do with the electronic communications of their customers and employees in the event of death.

As explained in excerpts within the September 1982 FOIA Update, Volume III, No. 4:

> "Can Exemptions 6 and 7(C) be applied to protect the privacy of deceased persons? No, not directly, but careful consideration should be given to whether such protection can be extended to others. After death, a person no longer possesses privacy rights...However, it is important to note that while privacy rights cannot be inherited by one's heirs, the disclosure of particularly sensitive personal information pertaining to a deceased person may well threaten the privacy interests of surviving family members or other close associates. "

Examples of cases where information about the deceased has been withheld when requested under the FOIA to protect survivors include:

- Hale v. United States Dep't of Justice, 1992, held there was "no public interest in photographs of the deceased victim, let alone one that would outweigh the personal privacy interests of the victim's family"

- Bowen v. FDA, 1991, affirmed nondisclosure of autopsy reports of individuals killed by cyanide-contaminated products
- Badhwar v. United States Dep't of the Air Force, 1987, information withheld noting that some autopsy reports might "shock the sensibilities of surviving kin"
- Marzen v. HHS, 1987, held the deceased infant's medical records exempt because their release "would almost certainly cause . . . parents more anguish"
- Isley v. Executive Office for United States Attorneys, 1998, approved withholding of "medical records, autopsy reports and inmate injury reports pertaining to a murder victim as a way of protecting surviving family members"
- Katz v. NARA, 1994; held that the Kennedy family's privacy interests would be invaded by disclosure of "graphic and explicit" JFK autopsy photographs
- New York Times Co. v. NASA, 1991, withheld the audiotape of voices of Challenger astronauts recorded immediately before their deaths, to protect family members from the pain of hearing the final words of loved ones
- Cowles Publishing Co. v. United States, 1990, withheld the identities of individuals who became ill or died from radiation exposure in order to protect living victims and family members of deceased persons from intrusive contacts and inquiries

However, such considerations do not always seem consistent in the findings of the courts. Each decision regarding the privacy of the deceased and protecting survivors is taken on a case-by-case basis. There are situations where information about the deceased will be released. For example:

- Outlaw v. United States Dep't of the Army, 1993, ordered disclosure in absence of evidence of the existence of any survivor who would be offended by release of murder-scene photographs of man murdered 25 years earlier
- Journal-Gazette Co. v. United States Dep't of the Army, 1990, held that because the autopsy report of an Air National Guard pilot killed in training exercise contained "concise medical descriptions of the cause of death," not "graphic, morbid descriptions," that the survivors' minimal privacy interest outweighed by public interest.

Privacy After Death and the U.S. HIPAA

In direct opposition to the U.S. Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA) provides that the right of privacy lasts beyond death. As explained in the Privacy Rule standard at §164.502 (f), covered entities must protect the privacy of deceased persons in the same way that the protected health information privacy is protected for the living. At §164.502(g)(4), the Rule goes on to require that "If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation." This certainly forces covered entities to think about how to handle the information of the deceased and address requests for such information.

Privacy After Death in Other Countries

The Unites States is not the only country for which the issue of privacy after death is something to contemplate. Multinational organizations need to be aware of the privacy rights of the deceased all over the world and adjust their procedures and policies accordingly. Just a few examples of such multinational rights include:

- As advised by the Office of the Federal Privacy Commissioner, the Australian Privacy Act of 1988 does not apply to deceased persons, or to any information, public or not, about deceased people. "However, the Privacy Act could apply if the information also includes or divulges personal information about a living person."
- Section 2(1) of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) states that 'personal health information' is information about 'living or deceased' individuals, while 'personal information' is information about an identifiable individual. Section 3(m) of the Canadian Privacy Act 1980 states that 'personal information' does not include information about an individual who has been dead for more than 20 years.
- In France the laws and subsequent judicial decisions appear to define privacy rights of individuals as all aspects of an individual's spiritual and physical being, giving in principle each person the power to define the boundaries of his/her private life and the circumstances in which private information may be publicly released. This right to privacy survives death, giving family members the ability to make privacy claims on behalf of the deceased.

Parting Thoughts…Pardon the Pun…

The right to privacy after death and survivors' privacy rights is an issue impacted by many potential laws and regulations, not to mention the ethical, humanitarian and practical considerations. This issue clearly demonstrates the need for people to take more responsibility for ensuring the privacy of their own information, and not just relying upon laws, service provider contracts, and others to do it for them. If you want someone to be able to read your email messages after your death, then give him or her your password so this type of situation can be avoided altogether. Of course, that person will then be able to access your email. And, the service provider's policy may not allow for "unauthorized" users such as this to use your email account. So, perhaps you should include the passwords to your email accounts, and following this train of thought, also to your other encrypted files, computer passwords, voice mails, and other password-protected information repositories, as part of your will for your designated beneficiaries to get upon your death, if this truly is what you want to happen. But, if you do this, then you will need to change your will every time you change your passwords. Perhaps a better alternative would be to indicate within your will where your passwords can be found, such as in a safety deposit box, and then be sure to keep your passwords there up-to-date. If you want to maintain privacy over certain aspects of your life after you die, then you need to be proactive and plan to ensure your privacy lives beyond your death as you wish. Consider speaking with your lawyer about these issues.

Is There Privacy Beyond Death?

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI

Written February, 2005
First Published in the CSI March 2005 Alert

Just telling people to be responsible for their own privacy is not enough. Organizations that possess personally identifiable information, as well as electronic "possessions" such as email messages, should educate their customers and employees about their personal responsibilities for maintaining privacy, and they should also consider privacy after death dilemmas. Think of the potential "close associates" whose lives could be dramatically affected by disclosure of relationships, loans, children, crimes, assets, and so on. Do surviving relatives have a right to read their deceased son's, daughter's, husband's or wife's communications with people whose lives could then subsequently be completely altered as a result? Who should make that decision? When should that decision be made? What will the courts do when surviving relatives start suing each other over disclosures about the recently departed? I know what it is like to be profoundly impacted by the loss of loved ones, and such grief often propels you to want to hang on to everything possible about and associated with them. However, such deep grief does not necessarily give survivors a right to everything about the deceased. If a person established controls to prevent others from seeing their information while they were alive, it is likely they did not want anyone to have access to it, even in the event of his or her death. This issue will not rest in peace any time soon.

Some actions your company should make before you get into a similar predicament as Yahoo! faced include:

- Identify any laws and regulations that apply to your company concerning how to manage the personal information and service information, such as email and messages, in the event of death.
- Consider all issues, make a decision and clearly document what you will do with the information of deceased customers and employees.
- Write supporting policies and procedures to reflect your decisions.
- Periodically test to ensure the procedures are effective. You do not want to wait until a death occurs to discover your processes do not work as envisioned.

Learn as if you were going to live forever. Live as if you were going to die tomorrow.
--Mahatma Gandhi

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is owner and principal of Rebecca Herold & Associates, LLC and can be reached at rebeccaherold@rebeccaherold.com. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," authored "Managing an Information Security and Privacy Awareness and Training Program" and is currently working on her 12th book. Rebecca creates "Protecting Information" and provides "Security Search" training at www.privacygudance.com

---