Hastings Law Journal

Volume 62 | Issue 4 Article 5

3-2011

Note – Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?

Molly Wilkens

Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?

MOLLY WILKENS*

The Internet has transformed the way we live our lives. What we have not yet fully realized is how it will impact what happens after we die. Specifically, the migration of financial services online, and the corresponding elimination of paper records, will hamper access to a decedent's financial assets and may eliminate knowledge of their existence entirely. This Note explores how federal financial and internet privacy laws affect the disclosure of a person's private financial information and offers solutions for reconciling lifetime privacy interests and the desire for access after death.

* J.D. Candidate, University of California, Hastings College of the Law, 2011; B.S. Brain & Cognitive Science and Writing, Massachusetts Institute of Technology, 2008. I would like to thank Professor Elizabeth Hillman for her guidance and thoughtful feedback throughout this process. Thank you also to James B. Creighton for sharing his expertise in the areas of Wills, Trusts and Estates. Finally, special thanks to my husband, Chris Wilkens, and my father, Dave Jabas, whose commitment to computer security prompted my interest in this topic.

TABLE OF CONTENTS

> There is only one thing that is inevitable in life, and that is death. . . . Unfortunately, there is no way to cheat death. It visits us all, whether we want it or not. For some, death is expected and they have time to say their goodbyes and prepare. For others, death can come quickly and unexpected[ly].[1]

INTRODUCTION

As financial transactions move online, hard copies now often form only a small fraction of a person's records. Paper bank statements, checkbooks, credit card bills, and receipts are being replaced by e-

1. JOHN N. PERAGINE, JR., THE COMPLETE GUIDE TO ORGANIZING YOUR RECORDS FOR ESTATE PLANNING: STEP BY STEP INSTRUCTIONS 15 (2009).

statements, online accounts, and confirmation emails. Documents once found in wallets, desks, and safety deposit boxes are now accessed mainly through email and website accounts.

Though online transactions are convenient for account holders during life, finding and understanding electronically-stored financial information after their deaths can quickly become a nightmare. There may be multiple computers or external hard drives that contain sensitive information. Online financial institutions keep transaction records and personal information as well: bank and investment websites, PayPal,[2] subscription services, electronic medical records, shopping websites, and membership services all hold customers' personal information. Customers often use one or more email accounts to receive updates from and communicate with these organizations. Each organization that collects a person's private information, including email service providers, may have different passwords, security questions, and personal identification numbers required to access the account. "If [a person does] a great job on security, [he] all but guarantee[s] no one can get easy and timely access to [his] digital world" in the event of death or incapacity.[3]

Nearly half of all adults with internet access in the United States use the Internet to bank or pay bills.[4] Online banking is equally common among all adult age groups under sixty-five.[5] "[P]eople are increasingly turning to Internet banking because of the high convenience, independence, and the typically better value it can offer."[6]

However, increased convenience comes with a price: privacy invasions and identity theft. For example, of the individuals whose checking accounts were compromised in 2004, 70% conducted financial transactions online.[7] Government reaction to this threat has been swift:

---

2. According to their website, "The service allows members to send money without sharing financial information, with the flexibility to pay using their account balances, bank accounts, credit cards or promotional financing." *Who We Are*, PAYPAL, https://www.paypal-media.com/who (last visited Mar. 31, 2011).

3. Dennis Kennedy, *Estate Planning for Your Digital Assets*, LAW PRACTICE TODAY (Mar. 2010), http://www.abanet.org/lpm/lpt/articles/ftr03103.shtml.

4. Liz Pulliam Weston, *Keep Thieves Out of Your Bank Account*, MSN MONEY, http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/KeepThievesOutOfYourBankAccount.aspx (last visited Mar. 31, 2011) (noting that 45% of adults with internet access bank or pay bills online); *Americans Heavily Press on Online Banking*, ECOMMERCE JOURNAL (Mar. 16, 2009, 8:58 AM), http://www.ecommerce-journal.com/news/13961_by_2011_76_of_americans_are_expected_to_turn_to_e_banking (explaining that an HSBC Direct report indicates that nearly half of all Americans age forty-five to sixty-nine use online banking).

5. Susannah Fox & Jean Beier, *Surfing to the Bank*, PEW INTERNET & AM. LIFE PROJECT (June 14, 2006), http://pewresearch.org/pubs/31/surfing-to-the-bank; *see also Americans Heavily Press on Online Banking*, *supra* note 4.

6. *Americans Heavily Press on Online Banking*, *supra* note 4.

7. Weston, *supra* note 4.

Congress passed laws punishing identity theft,[8] and the President created task forces to combat it.[9]

Existing financial regulations delineate with whom and under what circumstances financial institutions may share customers' private information.[10] These laws also create criminal liability for stealing private financial information.[11] Privacy laws, such as the Gramm-Leach-Bliley Act of 1999 ("GLBA")[12] and the Right to Financial Privacy Act of 1978 ("RFPA"),[13] protect customers of financial institutions from misappropriation and misuse of their nonpublic financial information.[14]

Online financial transactions and communications are additionally subject to internet privacy laws. The Electronic Communications Privacy Act of 1986 ("ECPA") prohibits companies that process, handle, and intercept electronic communications from knowingly divulging the contents of the communications.[15] Further, it prohibits electronic communications service providers from intentionally disclosing the contents of communications to any party other than the sender or the designated recipient.[16]

But the law can only do so much. Those who use online financial services must protect themselves, too. Privacy advocates advise consumers to treat any information they put on the Internet as inherently public.[17] Consumers are encouraged to have long, complicated passwords, to change them often, and to keep them secret.[18] Though effective for

---

8. *See, e.g.*, 18 U.S.C. § 1028A (2006).

9. *See generally About the Task Force*, IDTHEFT.GOV, http://www.idtheft.gov/about.html (last visited Mar. 31, 2011).

10. *See, e.g.*, 15 U.S.C. §§ 6801–6809, 6821–6827 (2006).

11. *See id.* §§ 6821–6827.

12. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).

13. Pub. L. No. 95-630, 92 Stat. 3697, 3707 (1986) (codified as amended at 12 U.S.C. §§ 3401–3422 (2006)) (giving customers a right to some level of privacy from government searches).

14. 15 U.S.C § 6801 ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. . . . [Financial institutions have an affirmative duty] to protect against any anticipated threats or hazards to the security or integrity of such records; and . . . to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.").

15. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

16. 18 U.S.C. §§ 2510–2522, 2701–2710, 2711 (2006).

17. GEORGE B. DELTA & JEFFREY H. MATSUURA, LAW OF THE INTERNET § 9.02, at 9-26 (3d ed. 2009) ("The best rule of thumb for all users of Internet-based communications systems is to assume that the content of their messages is not private."); *id.* § 9.03, at 9-38 (explaining that privacy problems also arise as a result of "information Web users knowingly and deliberately make available," such as online résumés and credit card information). For a list of good security habits created by the federal government, see ONGUARD ONLINE, STOP THINK CLICK: SEVEN PRACTICES FOR SAFER COMPUTING (n.d.), *available at* http://www.onguardonline.gov/pdfs/stopthinkclick_pl.pdf.

18. ONGUARD ONLINE, *supra* note 17, at 10.

maintaining privacy during life, following this advice often frustrates efforts to understand a person's financial situation after death.

When a person dies, probate laws facilitate the winding up of financial affairs.[19] The laws of intestacy govern what happens to property if a person dies without a will.[20] These are the "default rules."[21] If a person dies with a will, however, the will governs the distribution of his or her estate.[22] A will can also designate guardians for minors, decide which person or company will administer the estate, and achieve tax savings.[23] Despite the benefits of a will, 58% of American adults do not have one, leaving them with little input or control over what happens to their assets after death.[24]

As more people leave behind only electronic records, it will become increasingly difficult to effectively administer estates. Current internet and financial privacy laws inhibit the probate process, because the prohibitions on disclosure of private information make it nearly impossible for executors to access electronic communications and financial information.[25] Furthermore, establishing a succession plan for electronic assets seems to go "against every recommendation for good security practices," because sharing passwords gives access prematurely—trading lifetime privacy interests for ease of estate

---

19. *See* JESSE DUKEMINIER ET AL., WILLS, TRUSTS, AND ESTATES 39 (8th ed. 2009) ("Probate performs three core functions: (1) it provides evidence of transfer of title to the new owners . . . ; (2) it protects creditors by providing a procedure for payment of debts; and (3) it distributes the decedent's property to those intended after the decedent's creditors are pa*id.*" (emphasis omitted)).

20. *Id.* at 71.

21. *Id.* As a general rule, the law of the state where the person was domiciled at the time of their death governs the disposition of their personal property, and the state in which real property is located governs the disposition of real property. *Id.* at 72. This is true whether a person does with or without a will. *Id.* Thus, for example, if a person lived in Texas but had a vacation home in Florida, the vacation home in Florida would fall under Florida law, while the rest of their property such as books, furniture, and bank accounts would be dealt with under Texas law.

22. *Id.* at 71.

23. *Id.*

24. *Most Americans Don't Have a Will, Says New FindLaw.com Survey*, FINDLAW.COM (June 30, 2008), http://west.thomson.com/about/news/2008/06/30/findlaw-survey.aspx; *see also* DUKEMINIER ET AL., *supra* note 19, at 71 ("In spite of the many advantages of a will, roughly half the population dies intestate."). There are a variety of reasons why a person may die without a will: the time and cost involved, the idea that it's a "'big deal' to go to a lawyer," or the tendency to avoid thinking about one's own death. *Id.* at 71–72. "Nonetheless, underlying most individuals' failure to plan their estates is the frequently misguided belief that the law will take care of things in a satisfactory manner." RAY D. MADOFF ET AL., PRACTICAL GUIDE TO ESTATE PLANNING § 1.01 (2009 ed. 2008).

Furthermore, though incapacity may strike at any time due to accident or illness, "[r]esearchers generally report that less than 25% of people have [advance healthcare] directives, though some studies have found higher completion levels among selected groups with serious illnesses." DUKEMINIER ET AL., *supra* note 19, at 458 (quoting Rebecca Dresser, *Precommitment: A Misguided Strategy for Securing Death with Dignity*, 81 TEX. L. REV. 1823, 1829–30 (2003)). For an example of a young person struck by incapacity and the bitter family battles that followed, see *Bush v. Schiavo*, 885 So. 2d 321 (Fla. 2004).

25. *See infra* Parts II & III.

administration.[26] But having no plan at all creates uncertainty and delay in paying debts and distributing assets. Within the current framework, assets will remain frozen as executors attempt to locate and access financial assets held in online-only accounts.

This Note explores how federal financial and internet privacy laws affect the disclosure of a person's private information after death and the challenge of accessing online financial accounts at that time.[27] Recent scholarship on the digitalization of private life and its effects on probate focuses on nonfinancial assets, such as email, and the accompanying questions of ownership.[28] This Note focuses on financial assets, which are unencumbered by ownership issues, yet implicate overlapping state and federal regulations. Part I explains the current framework of probate administration and how assets held in online-only accounts complicate the procedure. Part II explores how financial regulation and internet privacy laws focus on lifetime privacy without providing for access after death. Part III reviews early proposals that have fallen short, because they do not provide privacy and access when desired. Finally, Part IV offers solutions for how online-only financial assets should be treated under the laws of financial regulation, internet privacy, and wills and intestacy, and proposes ideas for working within the current framework in the meantime.

---

26. Kennedy, *supra* note 3.

27. The interplay between federal law and probate proceedings is a complex area that, for the most part, lies outside the reach of this Note. The probate exception is "a judicially created limitation on federal court subject-matter jurisdiction that prohibits the exercise of jurisdiction over probate cases even where all the prerequisites for diversity jurisdiction are otherwise present." 32A AM. JUR. 2D *Federal Courts* § 795 (2010). The exception "has the effect of excluding most probate and probate-related matters from federal court." Peter Nicolas, *Fighting the Probate Mafia: A Dissection of the Probate Exception to Federal Court Jurisdiction*, 74 S. CAL. L. REV. 1479, 1482 (2000). Much uncertainty surrounds the scope of the probate exception to federal jurisdiction. It is often described as "one of the most mysterious and esoteric branches of the law of federal jurisdiction." Dragan v. Miller, 679 F.2d 712, 713 (7th Cir. 1982). For a comprehensive analysis, see Nicolas, *supra*, and also generally Allison Graves, Marshall v. Marshall: *The Past, Present, and Future of the Probate Exception to Federal Jurisdiction*, 59 ALA. L. REV. 1643 (2007).

28. *See generally* Justin Atwater, *Who Owns E-mail? Do You Have the Right to Decide the Disposition of Your Private Digital Life?*, 2006 UTAH L. REV. 397 (elucidating various arguments as to who owns email and suggesting how email should be treated under the laws of wills and intestacy); Jonathan J. Darrow & Gerald R. Ferrera, *Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?*, 10 N.Y.U. J. LEGIS. & PUB. POL'Y 281 (2007) (surveying various understandings of who owns email and proposing an analogy to bailment to describe the relationship between email account holders and email service providers); Olivia Y. Truong, *Virtual Inheritance: Assigning More Virtual Property Rights*, 21 SYRACUSE SCI. & TECH. L. REP. 57 (2009) (exploring the concept of "virtual inheritance" in the context of the virtual reality gaming industry).

I. Estate Administration

Executors[29] must have knowledge of an account's existence and access to that account to fulfill their fiduciary duties. The executor of an estate should complete administration and distribute assets as quickly as possible:[30] "Creditors must be paid. Titles must be cleared. Taxes must be paid and tax returns audited and accepted by tax authorities. Real estate or a sole proprietorship may have to be sold."[31] In simple cases, this process can take twelve months.[32] In more complicated cases, it can last much longer.[33] However, before any of this can be done, an executor must have a complete and accurate understanding of the decedent's financial affairs—what was owned, where it is, to whom the decedent owed money, and, if possible, to whom the decedent wanted to give property.

A. The Estate Executor as Sleuth: Paper Trails

If a person dies with a will, she dies testate;[34] if not, she dies intestate.[35] In either case, her financial affairs need to be sorted out: Magazine subscriptions need to be stopped, bank accounts closed, debts paid. But very few people have a holistic view of their own affairs during life, let alone keep adequate records for someone else to be able to discern the situation after death.[36] A typical decedent will leave what amounts to a scavenger hunt for her executor.[37]

---

29. An "executor" is the person named in a will to administer the estate. Dukeminier et al., *supra* note 19, at 40. An estate "administrator" is appointed by a probate court when a person dies without a will, or when the executor is unable or unwilling to serve. *Id.* This person may also be called a "personal representative." *Id.* The administrator is usually selected from a statutory list of persons "typically in the following order: surviving spouse, children, parents, siblings, creditors." *Id.* Throughout this Note, I will use the term "executor" to refer to anyone administering an estate, regardless of how they came to that position (whether through appointment by will or by a court).

30. An executor is a fiduciary, and as such, "inventories and collects the property of the decedent; manages and protects the property during the administration of the decedent's estate; processes the claims of creditors and tax collectors; and distributes the property to those entitled." *Id.*

31. *Id.* at 45 (discussing the closing of an estate). For a summary of probate procedure, see *id.* at 42–45.

32. Interview with James B. Creighton, Esq., Certified Specialist, Estate Planning, Trust & Probate Law, in S.F., Cal. (Jan. 24, 2010).

33. A famous example involves Vickie Lynn Marshall, also known as Anna Nicole Smith, who alleged tortious interference with a prospective lifetime gift in trust from her husband, J. Howard Marshall. The litigation, which began in 1996, has reached the U.S. Supreme Court twice to date and is still ongoing, despite the deaths of both Anna Nicole Smith and the plaintiff, her husband's son Everett Marshall. *See* Marshall v. Marshall, 547 U.S. 293 (2006); *see also* Stern v. Marshall, 131 S. Ct. 63 (2010) (granting petition for writ of certiorari).

34. Dukeminier et al., *supra* note 19, at 71.

35. *Id.*; *see also* discussion *supra* note 21.

36. Interview with James B. Creighton, *supra* note 32.

37. *Id.*

First, an executor must "marshal the assets."[38] This requires locating, valuing, and inventorying the decedent's assets.[39] Tangible property, such as furniture, artwork, jewelry, books, and real property are often consolidated and easy to locate—either in the decedent's home, or in a bank safety deposit box.[40] Intangible property, such as bank accounts, investments, and insurance policies requires more searching.[41]

To accomplish this task, an executor makes a diligent search through the decedent's papers.[42] The executor will look for bank statements, copies of contracts and insurance policies, bills, and so forth.[43] The executor will collect the mail, look at the decedent's computer, and talk to friends and family to find out where the decedent kept important information.[44] Taxes provide invaluable assistance in understanding a person's intangible assets. For example, Form 1099-INT shows the interest earned on an account,[45] and in some cases, receipt of this form will be the first time an executor becomes aware of an account's existence.[46]

Mere knowledge of an account's existence is insufficient; an executor must have adequate access to fulfill her fiduciary duties. Financial institutions are concerned about identity theft, even when working face-to-face with a private party who wants access to another person's account.[47] At a minimum, therefore, an executor often must appear at the financial institution and present personal identification, a certified copy of the death record, and other relevant documents demonstrating status as executor.[48] Though not required, knowing more information about the account holder—such as date of birth, Social

38. *Id.*

39. *Id.*; *see also* Donna Litman, *Financial Disclosure on Death or Divorce: Balancing Privacy of Information with Public Access to the Courts*, 39 SW. L. REV. 433, 437 (2010) ("The inventory generally includes a list of all assets owned by the decedent at the time of death that are subject to administration and the fair market value of these assets at the date of death."); *see also* UNIF. PROBATE CODE § 3-706 (amended 2006) ("[An administrator] shall prepare and file or mail an inventory of property owned by the decedent at the time of his death, listing it with reasonable detail, and indicating as to each listed item, its fair market value as of the date of the decedent's death, and the type and amount of any encumbrance that may exist with reference to any item."). For a comprehensive discussion of inventory and appraisal, see 1 ALEX R. BORDEN ET AL., CALIFORNIA DECEDENT ESTATE PRACTICE § 13 (2d ed. 2009).

40. Interview with James B. Creighton, *supra* note 32.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

45. *Id.* For a sample 2010 1099-INT form, see *F1099int*, IRS.GOV, http://www.irs.gov/pub/irs-pdf/f1099int.pdf (last visited Mar. 31, 2011).

46. Interview with James B. Creighton, *supra* note 32; *see also* PERAGINE, *supra* note 1, at 12 ("I had cases [where] the only way the executor . . . learned of accounts . . . was by waiting for statements in the mail.").

47. Interview with James B. Creighton, *supra* note 32.

48. *Id.*

Security number, and the account number—strengthens the executor's credibility.[49] Knowing this extra information may help ease bank personnel's worries.[50] However, as identity theft becomes more prevalent, more safeguards may be put in place that would further inhibit executor access.

B. Electronic Assets: The Trail Goes Cold

Electronic records are more cumbersome than their paper counterparts: They are harder to find, harder to access, and harder to wade through. A person's online presence can quickly become unwieldy. She may maintain websites and blogs, have accounts on Facebook, Twitter, or other social media sites, or use online storage sites such as Flickr or Google Docs.[51] Shopping accounts on any number of retailers' websites contain a consumer's credit card information to make future visits and purchases easier. Additionally, many people have multiple email accounts,[52] which may be used to communicate with online retailers and financial institutions. Each of these accounts must be known, accessed, and eventually closed after a person dies.

Online financial transactions and admonitions to "go green" eliminate many of the important clues to a person's financial life that are essential to an executor's duties. Paper bank statements are not mailed to customers; rather, they are stored online at the provider's website, behind passwords, key codes, and security questions.[53] Without regular statements in the mail, the only hope of finding hard copies of these statements and transactions would be if the consumer printed out copies from a personal computer and stored them. But this behavior seems

---

49. *Id.*

50. *Id.*

51. For more information about these websites, see *About*, Twitter, http://twitter.com/about (last visited Mar. 31, 2011) ("Twitter is a real-time information network that connects you to the latest information about what you find interesting. . . . At the heart of Twitter are small bursts of information called Tweets. Each Tweet is 140 characters in length, but don't let the small size fool you—you can share a lot with a little space."); *About Flickr*, Flickr, http://www.flickr.com/about/ (last visited Mar. 31, 2011) ("Flickr . . . has two main goals: 1. We want to help people make their photos available to the people who matter to them. . . . [and] 2. We want to enable new ways of organizing photos and video." (emphasis omitted)); Facebook, http://www.facebook.com/facebook (last visited Mar. 31, 2011) ("Facebook helps you connect and share with the people in your life."); Google Docs, http://docs.google.com (last visited Mar. 31, 2011) ("Upload . . . files[,] . . . edit and view . . . docs from any computer or smart phone . . . and [engage in] [r]eal-time collaboration . . . ." (emphasis omitted)).

52. *How Many E-mail Accounts Do Americans Have?*, IT Facts (Dec. 17, 2008), http://www.itfacts.biz/how-many-e-mail-accounts-do-americans-have/12128.

53. *Online Bank Account Management: What You Can Do*, Bank of America, http://www.bankofamerica.com/onlinebanking/index.cfm?statecheck=CA&context=en&locale=&template=what_you_can_do (last visited Mar. 31, 2011).

contradictory to the reasons people move these transactions online in the first place: namely, to reduce clutter and simplify transactions.[54]

With no paper trail, marshaling assets becomes nearly impossible. A decedent may have important information stored on multiple computers—many people have at least one laptop and one or more desktop computers.[55] The typical computer user may back up data on USB flash drives, external hard drives, CDs, or DVDs.[56] Finding all of this hardware can be a challenge in and of itself, let alone understanding the organizational structure or content contained on each storage device. Much of the vital information will not even be on a person's computer—it will be in an email or stored online at a financial institution's website.

Accessing a decedent's electronic communications and website accounts is no small task. First, there is a plethora of places to look. Three-quarters of employed American adults have at least one personal email address, and 59% have at least one work email address.[57] Twenty percent of young adults have three or more email accounts.[58] Though many people use Microsoft Outlook and other email programs that download copies of emails to a person's computer, many more use web-based email services.[59] Second, although more locations may mean more chances of finding records, all of those places employ different security measures. For example, notifications that financial statements are ready for viewing are sent to the customer's email account of choice[60]—which often requires a separate password from that of the bank website. For the technology savvy person, these passwords will be random, eight to twelve characters long, and change every ninety days.[61] Whether the decedent did not share a password because of security concerns or simply never got around to it, the result is the same: no access. Without access to, or knowledge of, relevant email accounts, awareness of online financial transactions could disappear entirely upon the death of the account holder.[62] Furthermore, even if one were aware of the account, it

54. *See Americans Press Heavily on Online Banking*, *supra* note 4.

55. Kennedy, *supra* note 3.

56. *Id.*

57. *How Many E-mail Accounts Do Americans Have?*, *supra* note 52.

58. *Id.*

59. Mark Brownlow, *Email and Webmail Statistics*, http://www.email-marketing-reports.com/metrics/email-statistics.htm (last updated Dec. 2010) (citing Erick Schonfeld, *Gmail Nudges Past AOL Email in the U.S. to Take No. 3 Spot*, TECH CRUNCH (Aug. 14, 2009), http://techcrunch.com/2009/08/14/gmail-nudges-past-aol-email-in-the-us-to-take-no-3-spot/) (demonstrating that the four big email domains as of July 2009 attracted the following numbers of unique U.S. users: Yahoo! Mail, 106 million; Windows Live Hotmail, 47 million; Gmail, 37 million; and AOL Mail, 36.4 million).

60. *See, e.g.*, *Online Banking from Bank of America: Online Banking Overview*, BANK OF AMERICA, http://www.bankofamerica.com/onlinebanking/?context=en (last visited Mar. 31, 2011) ("Life is hectic. Sign up for Online Banking and receive account alerts via e-mail or mobile device.").

61. ONGUARD ONLINE, *supra* note 17, at 10.

62. Kennedy, *supra* note 3.

is unclear how to report a death or provide documentation to an online-only financial institution, such as ING Direct.[63]

Tax forms are becoming electronic as well. Although the 1099-INT form currently arrives by mail, other tax forms are already moving online. A person can already receive W-2 forms and file their taxes electronically.[64] However, this is currently an "opt-in" phenomenon.[65] If all relevant tax information is sent and accessed electronically, knowledge of and access to one's email account will become vital in order to properly inventory the financial assets of an estate. As it is, though tax forms such as the 1099-INT are received in the mail, if a person dies in May or June, an executor may not know about the existence of an online account until January or February of the following year, causing a significant delay.[66]

A delay may drastically change the distribution of one's assets by a will. If assets are located after the distribution has been made, for example, they will go to the remainder beneficiaries.[67] To illustrate this, suppose a person with a will has a list of ten people to whom she wants to give $10,000 each, with any leftover assets to go to her children. If the executor and family are unaware of a bank account containing $100,000, there may not be enough remaining assets to give each of those ten people $10,000. In this case, the assets will be distributed down the list until they run out, leaving the last few people, and the children, as remainder beneficiaries, with nothing. If that account with $100,000 is found after the estate has closed, all of the $100,000 will go to the children as remainder beneficiaries, and the last few people to whom the decedent intended to leave $10,000 each will still receive nothing.

Frozen or missing assets are equally problematic when a person dies intestate. A person who dies without organizing her financial affairs runs the risk that her family will endure problems while waiting for assets that have been frozen by the bank or the court system.[68] The family "could wait months or years for the money to be released, while still being responsible for paying the mortgage or other expenses."[69] In an ideal

63. *About Us*, ING Direct USA, http://home.ingdirect.com/about/about.asp (last visited Mar. 31, 2011) ("We do business online, over the phone, and by mail. Without the overhead and high operational costs of other banks, we can pass those savings onto Customers.").

64. *See, e.g.*, *Delivering Paperless W2's for 2008*, Infor, http://www.infor.com/company/webcasts/fmsarchive/financials-rwc/fmspaperlessw2 (last visited Mar. 31, 2011) (stating that, when offered, there has been widespread acceptance of paperless W2 forms, averaging an 80% participation rate).

65. *See, e.g.*, *Exciting W-2 News*, Univ. of Utah Fin. & Bus. Servs. (June 22, 2009), http://fbs.admin.utah.edu/index.php/2009/06/22/exciting-w-2-news/ ("Employees can elect to only receive their W-2 electronically!!" (emphasis omitted)).

66. Interview with James B. Creighton, *supra* note 32.

67. *Id.*

68. Peragine, *supra* note 1, at 16.

69. *Id.*

situation, a decedent would at least leave evidence of an account's existence as a starting point for an executor. But awareness does not grant access, and current privacy laws, enacted to protect against unwanted access, also impede executors in administering estates.

II. Protecting Privacy: Financial Regulation and Internet Privacy Laws

Protecting privacy bars access under too many circumstances. Extensive, overlapping federal and state privacy regulations create a minefield for financial institutions and other companies to navigate. These laws cover topics such as "[i]nternet privacy restrictions; [f]inancial privacy; [u]nauthorized access to networks and information; [w]iretapping and privacy in electronic communications; [i]dentity theft; [and] [d]ata security," to name a few.[70] Failing to comply can be expensive: Regulatory fines and penalties may be imposed, litigation may arise, and remedying noncompliance may require costly changes.[71] Furthermore, the potential loss of business that results from consumer trepidation after theft of consumer data can be staggering.[72] This minefield of regulation makes internet service providers and financial institutions hesitant to cooperate with executors: Giving access after an account holder's death to accounts that were private during life may expose these institutions to liability or violations of federal and state privacy laws.

A. Privacy Law as a Tool: Protection Against Identity Theft

The overriding purpose of privacy law is the protection of consumer information.[73] With such a lofty goal, it is no surprise that "financial data is one of the most heavily regulated types of data."[74] The data is extremely important; if improperly acquired, it is highly likely that the consumer will become a victim of identity theft.[75] The movement to online financial transactions and to entirely online financial institutions creates new challenges in protecting consumers' nonpublic information and subjects these institutions to even greater regulation.

---

70. 1 Andrew B. Serwin, Information Security and Privacy: A Guide to Federal and State Law and Compliance § 1:1, at 2–3 (2009).

71. *Id.*

72. *Id.*

73. *See, e.g.*, 15 U.S.C. § 6801 (2006) (noting that it is the policy of Congress that financial institutions owe a duty to protect the security and confidentiality of their customers' nonpublic information).

74. 1 Serwin, *supra* note 70, § 16:1.

75. *Id.*

1. Financial Privacy

Banks owe a duty of privacy to their customers.[76] This duty arises from piecemeal federal and state legislation,[77] the contractual relationship between the bank and its customer,[78] and case law.[79] A long line of cases establishes the expectation that "a bank should keep its own customers' affairs confidential."[80]

Though a right of privacy in one's bank records is not guaranteed by the Fourth[81] or Fifth[82] Amendments, several federal laws address the need for individual privacy in financial affairs. The RFPA[83] grants customers of banks and similar financial institutions certain notification rights that would not otherwise exist as a matter of due process.[84] The GLBA[85] imposes privacy and security regulations on financial institutions.[86] It establishes penalties for those who obtain customer information via fraud, and further restricts disclosure of consumers' nonpublic personal information to nonaffiliated third parties.[87] One form of fraud that financial institutions increasingly encounter is "pretexting"—obtaining information under false pretenses.[88] Though it

76. *See, e.g.*, LCR Techs. Inc. v. HSBC Bank USA, 831 N.Y.S.2d 233, 234 (App. Div. 2007) ("[T]here may exist a duty in New York that a bank keep a customer's banking transactions confidential . . . [but] . . . compliance with a judicially authorized subpoena immunizes it from liability for any required disclosures." (citations omitted)).

77. *See, e.g.*, 15 U.S.C. § 6801(a) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.").

78. *See, e.g.*, Barnett Bank of W. Fla. v. Hooper, 498 So. 2d 923, 925–26 (Fla. 1986) (recognizing a duty of confidentiality where a bank has established a confidential or fiduciary relationship with a customer); Taylor v. NationsBank, 776 A.2d 645, 654 (Md. 2001) (affirming that absent compulsion by law, a bank cannot make disclosures concerning a customer's account without the express or implied consent of the customer); Djowharzadeh v. City Nat'l Bank & Trust Co. of Norman, 646 P.2d 616, 619–20 (Okla. Civ. App. 1982) (holding a duty of confidentiality arises during loan application process).

79. For example, an appellate court in Illinois held that there is a constitutional right under the Illinois Constitution to privacy in one's bank records. *See* People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) ("Since it is virtually impossible to participate in the economic life of contemporary society without maintaining an account at the bank, opening a bank account is not entirely volitional and should not be seen as conduct which constitutes a waiver of an expectation of privacy.").

80. *See, e.g.*, Aaron Ferer & Sons Ltd. v. Chase Manhattan Bank, 731 F.2d 112, 123 (2d Cir. 1984).

81. U.S. CONST. amend. IV; *see also* United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that a customer has no privacy right to records held by the bank under the Fourth Amendment).

82. U.S. CONST. amend. V; *see also* Fisher v. United States, 425 U.S. 391, 400–01 (1976).

83. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697, 3707 (1986) (codified as amended at 12 U.S.C. §§ 3401–3422 (2006)).

84. 2 MILTON R. SCHROEDER, THE LAW AND REGULATION OF FINANCIAL INSTITUTIONS 18A-2 & n.12 (2009) (discussing *Miller*, 425 U.S. 435).

85. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).

86. 1 SERWIN, *supra* note 70, § 16:2.

87. 2 SCHROEDER, *supra* note 84, at 18A-3.

88. 1 SERWIN, *supra* note 70, § 15:1; *see also Pretexting*, FTC.GOV, http://www.ftc.gov/bcp/edu/

has only recently garnered meaningful attention,[89] precautions taken against this form of fraud can significantly hinder executors' ability to demonstrate their authenticity and the necessity of their requests for decedents' information.

The GLBA has far-reaching effects:[90] Virtually any person who interacts with a financial institution and any document created during that process meet the definitions set forth in the Act. In fact, "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution" must comply with the provisions of the GLBA.[91] A "financial institution" includes banks, savings associations, credit unions, insurance companies, and credit card issuers.[92] It defines a "customer" as any person "to whom the financial institution provides a product or service, including that of acting as a fiduciary."[93] A "document" means "any information in any form" and thus includes electronic data transmission and computer communications such as email.[94] Thus, the Act seems to regulate disclosures related to nearly all of a person's financial transactions.

Obtaining "customer information of a financial institution" about another person through fraudulent means violates the GLBA.[95] "Customer information" includes personally identifiable account information, such as a customer's account number, credit card number, personal identification number, account password, or account balance[96]—the very information that executors would need to locate and access a decedent's account and to fulfill their fiduciary duties.

Not all disclosures of customer information violate the GLBA. Congress created exceptions for situations involving a "legitimate reason for obtaining the customer information."[97] For example, law enforcement officials who obtain information in the course of their official duties and insurance companies conducting insurance investigations into criminal activity, fraud, or material misrepresentations under the authority of

---

microsites/idtheft/consumers/pretexting.html (last visited Mar. 31, 2011) ("Pretexting is the practice of getting your personal information under false pretenses.").

89. 2 SCHROEDER, *supra* note 84, at 18A-8.

90. *See generally Examination of the Gramm-Leach-Bliley Act Five Years After Its Passage: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 108th Cong. (2004) [hereinafter *Gramm-Leach-Bliley Hearing*] (debating the Act's effects, including enabling banks to enter into new business arenas, responding to consumer needs for privacy protection, increasing competition in the marketplace, and encouraging financial conglomerations).

91. 15 U.S.C. § 6827(4)(A) (2006).

92. *Id.* § 6827(4).

93. *Id.* § 6827(1).

94. *Id.* § 6827(3).

95. *See id.* §§ 6821–6823.

96. 2 SCHROEDER, *supra* note 84, at 18A-8 (quoting 15 U.S.C. § 6827(2)).

97. *Id.*

state law do not violate the Act.[98] Other exceptions include disclosures of information made public because of securities law and disclosures to private investigators hired for child support collection.[99] Financial institutions may make disclosures "to comply with Federal, State, or local laws, rules, and other applicable legal requirements,"[100] or to resolve customer disputes or inquiries.[101] Executors do not fall within any of these exceptions.

However, the GLBA does provide that disclosures may be made "to persons holding a legal or beneficial interest relating to the consumer or to persons acting in a fiduciary or representative capacity on behalf of the consumer."[102] Thus, it appears on its face that financial institutions may safely disclose a decedent's private financial information to an executor. Though this exception exists, it is unclear how many executors, or financial institution personnel with whom they interact, are aware of it. Many executors are close family members or friends, untrained in the law.[103] Similarly, the employees with whom they interact will likely be told just to follow bank policies and procedures and will not be aware of these laws themselves. Finally, the GLBA is only one of many overlapping regulations in this area, so unless all of them make exceptions for executors, it is unclear how effective this particular exception will be.

Other federal privacy laws divide disclosures of confidential information into two categories: disclosures to government and disclosures to private parties. The RFPA, which provides protection against disclosure of consumers' private information to the government, prohibits disclosure of nonpublic information to federal agencies without customer authorization, unless the disclosure is in response to either an administrative summons, a search warrant, a judicial subpoena, or a written request that follows the procedures set out in RFPA.[104] The Act also provides a list of over a dozen situations in which it has no effect.[105] Administering an estate is notably absent from the list of legitimate circumstances in which an agency or person, other than one affiliated with the financial institution, would need a customer's account information.

---

98. *Id.* at 18A-8 to 18A-9.

99. *Id.* at 18A-9 to 18A-10.

100. 15 U.S.C. § 6802(e)(8) (2006).

101. 1 SERWIN, *supra* note 70, § 16:3, at 1159.

102. *Id.*

103. *Finding the Executor FAQ—Estate Planning and Probate*, FINDLAW, http://estate.findlaw.com/estate-planning/estate-planning-overview/estate-administration-executor-faq.html?DCMP=KNC-Estate&HBX_PK=executor+responsibilities&HBX_OU=50 (last visited Mar. 31, 2011).

104. 12 U.S.C. § 3402 (2006); *see also* 1 SERWIN, *supra* note 70, § 16:63, at 1229.

105. 12 U.S.C. § 3413 (2006).

Private parties have extreme difficulty gaining access to confidential information through appropriate channels. Under all circumstances, the owner of the account must be notified when confidential information is being requested or shared. The GLBA, for example, provides explicit protection against people who try to gain access to personal, nonpublic information without the authority to do so.[106] Financial institutions may not disclose to nonaffiliated third parties a consumer's account number or access information communicated through email to the consumer.[107] To this end, financial institutions are required to establish security systems and procedures to protect the confidentiality of their customers.[108] Thus, financial institutions are on guard against private third parties trying to gain access to another person's account without permission. An employee may be highly skeptical of, and uncooperative with, a person claiming to be an estate executor for fear that it is simply another form of pretexting. Establishing legitimacy for executors through documentation and knowledge of the account holder's personal information is vital for smooth interactions with financial institutions.[109]

2. Privacy on the Internet

Electronic communications between a financial institution and its customers are further subject to internet privacy laws, such as the Electronic Communications Privacy Act.[110] Title II, the Stored Wire and Electronic Communications and Transactional Records Access Act ("Title II"),[111] which applies to the dissemination or review of stored communications,[112] is the provision most applicable to executors who need access to electronically-stored emails, bank statements, and the like.

---

106. 15 U.S.C. § 6821 (2006). For various arguments that the Act has not achieved this goal, see *Gramm-Leach-Bliley Hearing*, *supra* note 90.

107. 15 U.S.C. § 6802(d) (2006). However, financial institutions do not need consent to share with affiliates. *See id.* Many argue that this exception has been abused. For a criticism of the policy that allows sharing of nonpublic information between affiliates, see *Gramm-Leach-Bliley Hearing*, *supra* note 90, at 6 (statement of Travis Plunkett, Legislative Dir., Consumer Fed'n of Am.) ("Consumers have no control over the sharing of their confidential experience and transaction information if two separate parties enter joint marketing agreements to sell financial products, nor do consumers have any right to stop the sharing of any information among affiliates of financial institutions. Some financial institutions have hundreds of affiliates; others have thousands.").

108. 15 U.S.C. § 6801(b) (2006).

109. Interview with James B. Creighton, *supra* note 32.

110. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.); *see also* 1 SERWIN, *supra* note 70, § 7:4, at 325–26 (providing a brief overview of the ECPA). The purpose of the Act is to "protect the privacy of individuals and to provide remedies for the violations of this law." 1 SERWIN, *supra* note 70, § 7:10, at 328. Title I of the ECPA, the Wiretap Act, applies to the interception of communications in transit. *Id.* § 7:11, at 329 (citing 18 U.S.C. § 2510 (2006)).

111. 18 U.S.C. §§ 2701–2712 (2006).

112. 1 SERWIN, *supra* note 70, § 7:52, at 354.

The purpose of Title II is to prevent hackers from obtaining, altering, or destroying certain stored electronic communications.[113] The Act treats these hackers as "computer trespassers."[114] In general, it is a crime to procure a communication to which one was not a party.[115] Exceptions to this rule include procurement by court order, or if the originator or addressee of the communication consents to the disclosure.[116] Executors are not parties to the communications, but need access to them. The exceptions listed suggest that executors can only gain access via court order or by previous consent from the decedent, either via will or through forwarding of relevant emails during life.

Intentionally accessing a wire or electronic communication without authorization while the communication is in an electronic storage system violates Title II.[117] However, the statute does not define "authorization" in either the definitions section or in the provisions setting out these restrictions. Thus, it is unclear what kind of documentation a decedent would need to leave behind to authorize access to her accounts after death. As such, privacy laws leave questions of access after death largely unanswered.

B. Privacy Law as a Weapon: Barring Access After Death

Without clear legislative guidance, online service providers have erred on the side of protecting privacy, even after death. Email service providers, for example, have wielded privacy laws to bar access to decedents' accounts for executors and family members.[118] When Lance Corporal Justin Ellsworth was killed in 2004 in Iraq, his father requested that Yahoo! provide him access to his son's email account.[119] Yahoo! refused access because the father did not have a valid password.[120] The

---

113. *Id.* (citing 18 U.S.C.A. § 2512(1) (a)–(c) (West 2008)).

114. *See* 18 U.S.C. § 2510(21) (2006) ("[A] 'computer trespasser' . . . means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and . . . does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.").

115. *See* 1 Serwin, *supra* note 70, § 7:54, at 354–55.

116. *Id.* § 7:55, at 355. Recall that Microsoft Outlook and other similar programs download copies of electronic communications to one's personal computer. A recent case suggests that reviewing copies of emails stored on a laptop may not violate the ECPA. *See id.* § 7:12, at 331 (citing Angel v. Williams, 12 F.3d 786 (8th Cir. 1993)). Thus, an executor who gains access to a person's email files stored on a personal computer may be able to treat those files as equivalent to paper documentation for evaluating the legality of their access.

117. *See* 1 Serwin, *supra* note 70, § 7:54, at 354–55; *see also* 18 U.S.C. § 2510 (providing definitions as used in the ECPA); 18 U.S.C. § 2701 (2006).

118. *See* Atwater, *supra* note 28, at 400.

119. *Id.*

120. *Id.* at 401.

company cited its strict company policy and terms of service in doing so.[121] Yahoo! did comply, however, with a Michigan probate court order requiring it to provide access to the Ellsworth family.[122] Interestingly, Yahoo! emphasized that it was only complying with the court order in this instance, and said it would continue to treat user emails as private and confidential.[123]

If widespread, this behavior could detrimentally delay or impede estate administration. Without access to the email accounts through which a financial institution communicated with the decedent, an executor would likely have no access to e-statements with account numbers or contact information for the financial institution, and thus, no knowledge of an account's existence. Like their brick-and-mortar counterparts, online-only financial institutions will not trust a person asking questions about a customer's private information if that person does not demonstrate authorization to access that information. But overlapping federal privacy regulations make disseminating this information to an executor nearly impossible. Recall that financial institutions are not allowed to provide customer information to nonaffiliated third parties—including account numbers, access information, and personal identification numbers.[124] And though the original sender or designated recipient of an email can consent to disclosure under the ECPA,[125] this possibility is foreclosed when the original recipient is dead and the original sender is a financial institution whose disclosures are severely limited. Thus, neither the financial institution under the GLBA, nor the email provider under the ECPA can forward the communications between the financial institution and the customer to an executor or close family member. This combination of adherence to privacy policies among financial institutions and email service providers will delay estate administration and bar access to a person's funds.[126]

---

121. *Id.*

122. *Id.*

123. *Id.*; *see also* Darrow & Ferrera, *supra* note 28, at 282 (reviewing the Ellsworth case and noting that the Yahoo! Terms of Service "indicate that survivors have no rights to access the e-mail accounts of the deceased" and that "account holders must agree that the 'contents within [their] account[s] terminate upon . . . death.'" (alteration original) (quoting *Yahoo! Terms of Service*, YAHOO!, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited Mar. 31, 2011))).

124. *See* discussion of the GLBA *supra* Part II.A.1.

125. *See* discussion of the ECPA *supra* Part II.A.2.

126. To date, Connecticut is the only state that has statutorily provided for executor access to the e-mail accounts and messages of decedents. *See* CONN. GEN. STAT. § 45a–334a (2009) (defining "electronic mail service provider" and "electronic mail account" and instructing that electronic mail service providers shall provide "access to or copies of the contents of the electronic mail account" of a person domiciled in the state at the time of his or her death upon either a written request of the executor and a copy of the death certificate or upon court order).

III. Privacy and Access: Two Ships Crashing in the Night

The clash between privacy laws and estate administration is fast approaching. Though young people dominate the online population, the biggest increase in internet use since 2005 has been in the seventy- to seventy-five-year-old age group.[127] Nearly half (45%) of that age group is now online.[128] Twenty-four percent of internet users in the G.I. generation (those born in 1936 or earlier) bank online.[129] Banking online, however, has not outpaced the growth in internet use generally.[130] One reason for this may be the trust gap.[131] Banks must work to dispel the belief that financial information is not safe from identity theft online.[132] The increase in online banking among older generations illustrates the need for immediate attention and concern regarding the balance of lifetime privacy and access after death.

Current attempts to reconcile privacy during life and access after death fail to address the whole problem. Advocates of the highest level of privacy sacrifice the awareness and access critical to taking care of one's financial affairs after death. Estate planning shortcuts, on the other hand, largely disregard a person's lifetime privacy interests. Finally, all of these solutions require advanced planning, and therefore do nothing for the person who dies intestate.

A. Abandoned Property Statutes: A Last Resort

Advocates of lifetime security at all costs may note that, if all else fails, abandoned property statutes and procedures will bring awareness of secret or forgotten accounts. The problem with this approach is that all else *must* fail before these statutes take effect.

---

127. *See* Sydney Jones & Susannah Fox, Pew Internet & Am. Life Project, Pew Internet Project Data Memo: Generations Online in 2009, at 2 (2009).

128. *Id.*

129. *Id.* at 5.

130. *Id.*

131. *Id.*

132. *Online Banking Customers Attitudes and Activities*, eMarketer (Nov. 2005), http://www.researchandmarkets.com/reports/307805. *See generally* Bomil Suh & Ingoo Han, *Effect of Trust on Customer Acceptance of Internet Banking*, 1 Electronic Com. Res. & Applications 247 (2002) (finding that beyond beliefs regarding ease of use and usefulness, trust beliefs impact a person's acceptance of internet banking). Stolen wallets and physical paperwork account for 43% of identity thefts, whereas only 11% are accomplished using online methods. Carrie Davis, *Official Identity Theft Statistics*, SPENDonLIFE.com (July 8, 2009), http://www.spendonlife.com/guide/identity-theft-statistics. Bank of America is working to address this and to combat the "trust gap" by advertising online banking as a way to prevent identity theft. *Online Banking from Bank of America: Open an Internet Banking Account*, Bank of America, http://www.bankofamerica.com/onlinebanking/ (last visited Mar. 31, 2011) ("Lower your risk of identity theft and mail fraud by viewing copies of your checks online and stopping delivery of your paper statements.").

Property held by financial institutions that has not been accessed for a specified period of time is deemed "abandoned."[133] In California and Massachusetts, for example, property becomes abandoned when the owner cannot be contacted for a period of about three years.[134] State laws require businesses to review their records annually to determine whether they have abandoned property and if so, to report it to the state.[135] When the state's abandoned property division receives the property, the division sends a notice to the owner's last known address and enters property information into a searchable online database.[136] The assets are held in perpetual trust for the true owners.[137]

Online-only financial institutions, such as ING Direct, are required to turn over abandoned property to the state of the owner's last known address.[138] To prevent abandonment, ING Direct suggests that customers log into their accounts, call on the phone, or interact with an associate at least once per year.[139] The financial institution is required to make a "diligent effort" to contact the owner before handing over the property to the appropriate state abandoned property division.[140] To comply with this requirement, ING Direct uses the email and mailing addresses on file for a customer to send the customer email notifications and a state-mandated letter warning the customer of impending escheatment before turning the property over to the State.[141] However, because these "diligent efforts" only require contacting a person through email and mail, an executor may not become aware of the property until it has escheated to the State for the same reasons as brick-and-mortar financial institutions. That is, if the executor does not have access to the decedent's account, the executor will not receive the email notifications. Furthermore, if email service providers, like Yahoo!, insist that they can

133. *See, e.g.*, *What Is Unclaimed Property?*, CAL. STATE CONTROLLER'S OFFICE, http://www.sco.ca.gov/upd_faq_consumer_about_q01.html (last visited Mar. 31, 2011); *see also Frequently Asked Questions*, MASS. ABANDONED PROPERTY DIV., http://abpweb.tre.state.ma.us/abp/abp_faq.htm (last visited Mar. 31, 2011).

134. *Frequently Asked Questions*, *supra* note 133; *What Is Unclaimed Property?*, *supra* note 133. In many states, there are separate abandoned property law provisions governing safety deposit boxes. For a comprehensive survey of applicable state laws, see WESTLAW 50 STATE STATUTORY SURVEYS: FINANCIAL SERVICES: BANK OPERATIONS—SAFE DEPOSIT BOX REQUIREMENTS (2009). The contents of a safety deposit box are deemed abandoned after anywhere from one to seven years of nonuse, with five years being the most common timeframe. *Id.*

135. *See Frequently Asked Questions*, *supra* note 133.

136. *Id.*

137. *Id.*

138. *Unclaimed Property*, ING DIRECT, http://helpcenter.ingdirect.com/ (follow "Help Topics" hyperlink; then follow "Unclaimed Property" hyperlink) (last visited Mar. 31, 2011) ("ING DIRECT is required (under State laws) to turn over those funds to the State of the Customer's last known address.").

139. *Id.*

140. *Id.*

141. *Id.*

terminate an email account at the death of its owner and delete all the contents of that account, all electronic statements and communications between the decedent and the financial institution will be erased before ING Direct would even send that email notification.[142]

A delay of three years can be costly. Three years after a person dies, an executor may not receive the notice in the mail—the post office's mail forwarding service only lasts for a period of months, and if the property at which the decedent lived was sold, the notice may never get to the right people. Thus, it would seem that reliance on abandoned property statutes to solve the privacy-access conundrum would create an ongoing obligation that executors check the searchable database[143] for accounts that may show up after the estate has been closed. Under current probate laws, however, when an estate is closed, the executor's fiduciary duties end. Thus, adding a duty that extends beyond the closing of the estate itself would complicate defining the end point of estate administration.

B. Sharing Passwords: A Risky Undertaking

Because relying on abandoned property statutes is an unappealing last resort, estate planning attorneys often advise clients to create a list of accounts and passwords to keep with other important documents.[144] But sharing passwords comes with its own set of problems: namely, organizational issues, outdated information, and premature access to accounts.

Organizing electronic information for others to access later requires a different approach than the paper paradigm. With paper records, a person could easily create awareness of an account without granting access. Records could be kept in a central location, such as in a safe or filing cabinet at home, a safety deposit box at a bank, or with a trusted third party such as a financial advisor.[145] To share that information, a person simply told others the location of the documents. Re-creating this paper paradigm by printing and storing hard copies of documents requires time and persistence; thus, few utilize this option.

Creating awareness without granting access becomes more complicated with electronic documents, because the documents are

---

142. *See* Darrow & Ferrera, *supra* note 123, at 282.

143. Many states have online searchable databases for abandoned property. *See, e.g.*, *Unclaimed Property Search*, Cal. State Controller's Office, http://scoweb.sco.ca.gov/UCP/ (last visited Mar. 31, 2011).

144. Interview with James B. Creighton, *supra* note 32; *see also* Kennedy, *supra* note 3, at 4–5 (advocating keeping a list of passwords and telling others where that list is located).

145. *See* Kennedy, *supra* note 3 ("Most of us keep important papers, necessary information and valuable assets in safe places. These places are usually revealed to a few trusted people who we hope also survive us.").

stored either on the Internet or on a personal computer. To avoid the burden of creating hard copies, a person may try to organize their digital records. Aptly labeled directories, folders, or documents on a computer can make it easier for loved ones to find important records—the equivalent of color coding and clearly labeling file folders in an office. However, keeping sensitive private information on a personal computer is inadvisable because of the risk of identity theft. It is not a good security practice to name folders and documents things like "'Passwords,' 'Important Financial Stuff' or 'Account Information' in case someone breaks into [the] computer system or steals [the] computer."[146] Though loved ones searching the directory for these terms would be able to find the relevant information quickly and easily, so would a computer hacker or a person who stole the computer itself. Thus, attempts to apply the old practices of writing things down or keeping copies do not easily translate to electronic transactions and recordkeeping. In fact, applying paper paradigms to computer recordkeeping may seriously compromise the privacy and security of one's records.

Without a reliable way to create awareness of an account while delaying access, one may simply decide to share passwords. "Options [for sharing passwords] include printing out a list, putting the information on a flash drive, or burning it onto a CD."[147] However, sharing passwords, rather than account statements, gives full access to others before they need it—before death or incapacity—and "[w]hoever has access to account information could take the money without being detected."[148] Additionally, full access creates a bigger sorting problem than traditional paper documents. The ease and volume of electronic storage has made these records more amorphous than their paper counterparts. For example, logging into a bank's website allows a person to view a list of transactions, PDFs of previous monthly statements, multiple checking and savings accounts, investments, and loan information, all at once.[149] Even if a person were to leave information on how to access these records, it would require continual updating as passwords and account information are changed. Thus, "[a]lmost by definition, any document that [one] create[s] will be out of date when the time comes to use it."[150]

146. *Id.*

147. Deborah L. Jacobs, *When Others Need the Keys to Your Online Kingdom*, N.Y. TIMES, May 21, 2009, at F2.

148. *Id.*

149. *Online Bank Account Management: What You Can Do*, *supra* note 53.

150. Kennedy, *supra* note 3.

C. Electronic Safety Deposit Boxes: Leaving Records but Delaying Access

In an attempt to reconcile privacy advocates' and estate administrators' interests, several commercial providers have stepped in to create online repositories for sensitive information. Services such as Legacy Locker[151] and Estate++[152] enable customers to store and update account information, and to have it released to certain designated people when particular events occur. Of course, these services come with a fee.[153] And though there are at least seven such competitors in the field, the services they provide vary widely.[154] Storage space varies from as little as one gigabyte to unlimited, pay-as-you-go storage.[155] Some, but not all, offer such security features as encryption, Open ID authentication,[156] and identity theft protection.[157]

These services fall short of providing a consistent way to reconcile privacy interests during life with access interests after death. First and foremost, they require advanced planning. Recall that in the United States, more than half of adults do not have a will.[158] These solutions do nothing for the decedent who dies intestate, leaving a smattering of disorganized paper records, if any at all. They do equally little for the decedent who dies intestate but diligently followed password and security guidelines during life.

Concerns of premature access and identity theft are left unresolved. If a person does not trust a close relative, friend, or financial advisor with a current list of passwords and account information, it seems even less likely that this person would pay a fee to a total stranger to keep that information online. With identity theft on the rise, it is not unfathomable that these repositories of personal information will be targeted just as much as financial institutions or individual consumers. David H. Holtzman, an internet security expert, notes, "There is not a company I

---

151. Legacy Locker, http://legacylocker.com/ (last visited Mar. 31, 2011).

152. Estate++ Virtual Safe Deposit Box, http://www.estateplusplus.com/ (last visited Mar. 31, 2011).

153. Legacy Locker, for example, offers a limited trial account, which allows three assets, one beneficiary, and one legacy letter. *Legacy Locker Plans*, Legacy Locker, http://legacylocker.com/signup (last visited Mar. 31, 2011). Customers may choose between paying a one-time fee of $299.99 or an annual fee of $29.99 for unlimited assets, unlimited beneficiaries, and unlimited legacy letters. *Id.* The fee versions also include document backup and video upload capabilities. *Id.* Estate++, on the other hand, has a $2, one-time sign up fee, a monthly fee of $1, and metered usage charges for data stored, transferred in, and transferred out. *Estate++—Subscribe Now!*, Estate++, http://www.estateplusplus.com/BuyNow.html (last visited Mar. 31, 2011).

154. *Compare Us to the Competition*, Estate++, http://www.estateplusplus.com/Competition.html (last visited Mar. 31, 2011).

155. *See id.*

156. OpenID Found., http://open*id*.net (last visited Mar. 31, 2011).

157. *See Compare Us to the Competition*, *supra* note 154.

158. *See Most Americans Don't Have a Will, Says New FindLaw.com Survey*, *supra* note 24.

know that I would trust with all my eggs in one basket."[159] In fact, more so than with giving access to a trusted person—who would be the primary suspect in the event of missing funds—giving all of one's information to a third-party company brings a significant risk of complete and irreversible exposure.

In some instances, the security features of online safety deposit products can work against the consumer. Legacy Locker's efforts to keep all data encrypted and inaccessible to people within the company makes it difficult to get such simple customer service as dealing with a forgotten password.[160] Furthermore, these online services rely entirely on the consumer to continuously update the information contained on these sites. This creates the same dilemma as continually updating a hard copy of the same information—people simply will not get around to it.

Finally, awareness issues remain with any online repository controlled by the decedent. Legacy Locker, for example, requires someone to notify the company that a person has died.[161] This requires knowing that the decedent had a Legacy Locker account in the first place. Most interactions with the company are conducted over the Internet, creating the same access and awareness issues as an online bank account where transactions occur via email. Legacy Locker does, however, attempt to create some sort of a paper trail. As part of a paid account, a customer receives a card directing any medical personnel or family members to contact Legacy Locker and "Report a Death."[162] Presumably, this card could be kept in one's wallet or in a safe place with other paper documents in the event of death or incapacity.

IV. Proposals: Privacy and Access Do Not Have To Be Mutually Exclusive

Although previous attempts to secure privacy during life or access after death have only looked at one part of the issue, these goals do not have to be mutually exclusive. Several courses of action exist for reconciling privacy interests and ease of estate administration.

A. Creating Statutory Access for Executors

Current federal privacy laws do not adequately address estate administration. While the GLBA makes exceptions for disclosing

159. Jacobs, *supra* note 147.

160. *See Legacy Locker Help*, Legacy Locker, http://legacylocker.com/support/help (follow "Password Security" hyperlink) (last visited Mar. 31, 2011) ("Your password information is stored in the same way as the rest of your data.").

161. *See id.* (follow "How do you know when I die" hyperlink) ("Someone will have to report your name to our system as being deceased.").

162. *See Frequently Asked Questions*, Legacy Locker, http://legacylocker.com/support/faq (follow "How do you know when I die?" hyperlink) (last visited Mar. 31, 2011).

customer information to estate executors, other federal privacy laws do not.[163] But, any person not described in the exceptions falls into the broad category of "nonaffiliated third parties," with whom financial institutions can share the least amount of information.[164] Estate executors should have more access than others who would qualify as "private parties" seeking access to an account. Congress could address this problem in several ways.

First, Congress could add executors to the limited list of exceptions for disclosures of electronic communications. Congress has already recognized in the GLBA that executors of estates have a worthy public purpose that should be protected.[165] If executors are not granted access to the electronic communications between a financial institution and its customer, they will not be able to make use of the exceptions in Title V of the GLBA.

Second, Congress could require a third instance of consent disclosure to be implemented by the financial institutions. The GLBA requires financial institutions to tell consumers about the institution's policies on the disclosure of nonpublic personal information to nonaffiliated third parties.[166] They are also required to allow consumers to "opt out" of disclosure of their information to nonaffiliated third parties.[167] However, because this "opt out" burden falls on the consumer, and because the disclosures required by the GLBA are often incomprehensible, few consumers actually opt out.[168]

The GLBA could further require financial institutions to gain customers' permission to disclose certain communications or financial information to an executor in the event of their death. To be effective, this should occur when the account is opened. With online accounts, a plethora of additional records may be available that would not have been available had the executor simply been given check-writing privileges for an account with a brick-and-mortar bank.[169] Customers could check boxes giving consent to particular types of disclosures, such as transactional information, account password reset privileges, backdating of statements, and so forth. For example, an executor likely does not need to see twenty-five years worth of statements in order to marshal the assets and pay debts. A person could allow access to the last twelve months of statements for their main checking account, but only allow the

163. *See generally* 1 SERWIN, *supra* note 70, § 16.

164. *See* discussion of federal privacy laws *supra* Part II.A.

165. *See supra* note 102 and accompanying text; *supra* Part II.A.1 (discussing exceptions for executors under GLBA).

166. 15 U.S.C. § 6802(a) (2006).

167. *Id.* § 6802(b).

168. *See Gramm-Leach-Bliley Hearing*, *supra* note 90, at 6 (statement of Travis Plunkett, Legislative Dir., Consumer Fed'n of Am.).

169. *See* 1 BORDEN, *supra* note 39, §10.10.

executor to see the balance of their savings account as of the date of death. Thus, customers could customize and protect their lifetime privacy interests after death if it would not be materially necessary to the estate administration process.

State legislatures could take similar measures to give access to executors. Much like the Connecticut and Oklahoma statutes granting executor access to a decedent's email account,[170] state laws could grant limited access to financial account information as well. State laws inconsistent with a provision of the GLBA are displaced by the federal law, but "only to the extent of the inconsistency."[171] Thus, the legislative changes suggested above could be implemented at the state level, without being superseded by the federal statute. Whether enacted at the state or federal level, these legislative changes are extremely important because they change the default rules, which most Americans eventually rely on to govern the administration of their estates.

B. Working Within the Current Framework in the Meantime

Executors need to be prepared for uncooperative financial institutions and email service providers. Some probate codes, such as California's, have provisions for executors to bring uncooperative institutions into court.[172] Recall that Yahoo! complied with the Michigan probate court's order to grant Justin Ellsworth's family access to his emails.[173] However, this should be a last resort for executors, because litigation is expensive and time consuming.

Financial institutions need not hide behind federal privacy laws when an executor legitimately needs access to an account and asks for it through appropriate channels. It is not an unauthorized disclosure under the GLBA when a password or personal identification number is given to a third party with the customer's consent.[174] Furthermore, a financial institution will not violate the GLBA if it discloses a customer's nonpublic information "to comply with Federal, State, or local laws, rules, and other applicable legal requirements."[175] Following a probate court order, for example, would fall within this category.

---

170. Conn. Gen. Stat. § 45a–334a (2009); Okla. Stat. tit. 58, § 269 (2010).

171. 15 U.S.C. § 6807(a) (2006); 2 Schroeder, *supra* note 84, 18A-13 ("The savings clause specifically validates state laws—whether statutory, administrative, or judicially based, that provide any person protection greater than the protection under [the GLBA]."). *Contra Gramm-Leach-Bliley Hearing*, *supra* note 90, at 10 (statement of Steve Bartlett, President & Chief Exec. Officer, Fin. Servs. Roundtable) (arguing that this savings clause should be eliminated and that Congress should use the GLBA to create a national privacy policy).

172. *See* Cal. Prob. Code § 850 (West 2002).

173. *See* Atwater, *supra* note 28, at 400–02 (discussing the case of Justin Ellsworth).

174. *See* 2 Schroeder, *supra* note 84, at 18A-17.

175. 15 U.S.C. § 6802(e)(8) (2006).

Those who bank online likely only communicate with those banks electronically, via email.[176] However, email service providers routinely refuse to cooperate with relatives or executors, arguing that they have a duty to protect the privacy of their users.[177] The ECPA restricts disclosure to governmental entities of transactional data associated with electronic communications but authorizes disclosure of such information to private parties.[178] Transactional data includes email addresses, billing information, and data regarding frequency of use.[179] Thus, in response to an executor's query of whether or not a decedent had an account at an online financial institution, such as ING Direct, the financial institution could reasonably disclose the email address it used to communicate with the decedent and to confirm that the financial institution does have an account in the decedent's name. These small pieces of information could dramatically help an executor without compromising the account holder's privacy.

C. Expanding Estate Planning Practices to Consider Electronic Assets

Estate planning attorneys know the importance of asking the right questions to find the information they need. Initial questionnaires with clients should take into account the electronically stored aspects of a client's life—investment and bank accounts, social networking sites, pictures stored online, blogs, and email. Attorneys should be familiar with the barriers to access after a person dies and should educate clients about what types of electronic assets they should take care to pass on during life. For example, many email service providers will not give access to the contents of emails to family members after a person dies.[180] Thus, if one's client wants to pass on access to sentimental things stored online, they should plan to have joint access to these accounts—or share their passwords with someone they trust—sooner rather than later.

Estate planning attorneys will need to decide what framework works best for their client's needs. Dennis Kennedy, an information technology lawyer, explains an example of how to create a record of one's digital assets: (1) inventory the digital assets, (2) identify appropriate help, (3) provide for access, (4) provide instructions, and (5) give appropriate authority.[181] This is a great place to start, but without exceptions in the federal privacy laws for estate executors, probate

176. Banks encourage this. *See, e.g.*, *Online Banking from Bank of America: Online Banking Overview*, *supra* note 60.

177. *See* discussion of the Ellsworth case *supra* Part II.B.

178. 18 U.S.C. § 2703(c) (2006).

179. Delta & Matsuura, *supra* note 17, § 9.01, at 9-7.

180. *See* Atwater, *supra* note 28, at 400–02 (discussing the case of Justin Ellsworth).

181. *See generally* Kennedy, *supra* note 3.

administration will become an increasingly difficult and burdensome task, even with the most proactive client.

CONCLUSION

Online banking and other financial transactions are here to stay. Their popularity is increasing, not only amongst younger generations, but also amongst retirees. Despite disappearing paper trails, courts have not yet needed to address on a large scale the conflicts of privacy laws and probate administration. This is partly due to the lag between the introduction of these types of transactions and the deaths of those who use these services most. The number of internet users who conduct financial transactions online is increasing in every age group. As time moves forward, more and more people who die will have multiple email accounts, online financial services providers, and diminishing paper records. This has already become a pressing legal issue and it will only become more so in the coming years.

Though privacy laws and probate laws both have admirable goals, they currently conflict with one another. There are several potential solutions for effectively giving access to estate executors while protecting the lifetime privacy interests of individuals. Until the law catches up, estate planning attorneys need to be mindful of access and awareness difficulties and address online financial assets with clients.