BOVE&LANGA
LAW FIRM

Ten Tremont Street, Suite 600 | Boston, MA 02108
www.bovelanga.com | p 617.720.6040 | f 617.720.1919

THE TRUSTWORTHY ADVISOR

ASSETS FROM SPACE – CYPERSPACE, THAT IS! THE NEW FRONTIER OF ESTATE PLANNING

PART ONE

Alexander A. Bove Jr. and Melissa Langa

Planning for special assets and changes in the law brought about by social and technological advances poses a constant challenge to estate planners. For example, suddenly, it seemed, real estate became condominiums and cooperatives, and trusts were not only for people. Now we must learn to deal with electronic digital assets. And sometimes the means of access to a digital asset seems like an asset in itself.

Online multiplayer game accounts, social networking and dating sites, e-mail accounts, iTunes, Twitter, bitcoins, DropBox, rewards programs, Instagram, airmiles, blogs, PayPal, domain names, electronic banking, electronic accounting programs – these are just a few of the new digital assets and accounts clients are bringing into our conference rooms. And with them come a host of planning issues in addition to access, including identification, privacy, drafting considerations, and, in some cases, valuation. In Part One of this Advisory, we will discuss identification and access issues. In Part Two, we will discuss drafting and valuation issues.

A New Yorker cartoon recently showed a man standing on a cloud in front of St. Peter, who was guarding access to the pearly gates of Heaven. St. Peter growls at him: "What was the name of your first pet?" Gaining access to a client's digital assets may not be the same as gaining access to heaven – it just might be harder. But first, you must know where to look. This is where record-keeping by the client is of vital importance. In the ideal world, each client will create a "Personal Inventory" of all assets, including a separate schedule of digital assets, with access instructions. We provide such a document to our clients as part of the planning process. But the existence of a

personal inventory itself raises issues. In addition to the terrible burden of keeping the inventory current, the client must protect the inventory from criminals and peeping Toms.

A list of all a client's active digital assets with accompanying URLs, passwords, usernames, PINs, and the answers to the "secret questions" is a formidable document, a powerful planning and estate administration tool, but who should be the keeper of this document – the key to Heaven – is not easily answered. Should the lawyer hold the key? Ethical rules governing the practice of law already impose a duty to carefully guard the privacy of a client's file, and you might think that adding one more document to the file should not be too great a burden to undertake. Before agreeing to do so, however, the lawyer must carefully consider the potential liability which might attach should the lawyer or a member of lawyer's firm carelessly leave a file on the desk overnight, or in an unlocked file cabinet, and the personal inventory falls into the hands of person who harms the client with this information.

There are companies which provide software to manage passwords and the like, such as 1Password and RoboForm; and companies which store a client's digital asset information and divulge it only to those individuals who are named by the client, such as DeathSwitch. The risk here is that given the nature of the service provided, these companies are natural targets of a hacker who slips in between the cracks of the company's security systems.

There is no easy answer to this issue of where the personal inventory is kept, but perhaps the best place might be in a safe deposit box. The overly cautious client without trusted family members will grant nobody access to the box until death, requiring probate to be opened and the appointment of a personal representative.

Even if the legal representative is able to locate and gain access to a digital asset, is it a good idea? There are two main laws which impact estate planning with digital assets: (i) the Stored Communications Act, 18 U.S.C. §2701 et. seq. (protects against the unauthorized disclosure of certain electronic communications); and (ii) the Computer Fraud and Abuse Act (and corresponding state laws), 18 U.S.C. 1030 (protects against unauthorized use of protected computers). The recent case of *Ajemian v. Yahoo!,* 987 N.E.2d 604 (Mass. 2013) illustrates how these laws might hinder the ability of a legal representative to access a decedent's Yahoo! email account, and it is recommended reading for all trusts & estates lawyers. Suffice it to say that

states have begun to enact legislation to address the access issue, and Delaware in 2014 was the first state to enact the Uniform Fiduciary Access to Digital Assets Law. Closer to home, a Massachusetts House Bill No. 4243 would amend the Uniform Probate Code M. G. L. chap. 190B, section 3-715 (Transactions authorized for personal representatives; exceptions) to grant a personal representative broad powers over electronic records. One hopes that if the Massachusetts legislature is serious about addressing the problem of access to digital assets a concurrent amendment will be made to the powers granted a trustee under the Massachusetts Uniform Trust Code, M.G.L. chap. 203E.

In addition to statutory obstacles to access, there are also contractual restrictions to contend with. Each digital asset comes with its own "terms and conditions" which the client has possibly agreed to by clicking through to open the desired digital account. These contractual restrictions are often formidable, and should be read prior to attempting access.

So how does the lawyer put it all together? As always with estate planning, by asking careful questions to develop the facts and understand the client's goals, and by drafting documents which take this information and produce a plan which implements these goals. These issues are addressed in Part Two.