Dropbox Security Concerns?

You may have read or heard about recent security concerns involving Dropbox, the wildly popular file sharing service. Thanks to several Twitter friends, I was directed today to this excellent post by Michael Kassner at Tech Republic. Here is the back story:

> Two highly-skilled researchers Derek Newton and Christopher Soghoian have issues with Dropbox. Newton stumbled onto a viable attack vector and Soghoian found serious inconsistencies in the Dropbox privacy policy.
>
> I use Dropbox. And, when security researchers I'm familiar with publically post warnings, a bomb goes off in my head. Besides, I know many people who use Dropbox.
>
> So, like all good journalists–particularly those with grandfathers like mine–I feel obligated to gather the facts as presented by all parties. To that end, I contacted Dropbox. The following questions were answered by ChenLi Wang, Business Operations at Dropbox.

Read the full post here.

What does the Oregon State Bar have to say on the subject of confidentiality, security, and file sharing in the cloud? We have no formal opinion, but Helen Hierschbiel's article, Odds & Ends: Safeguarding Client Information in a Digital World, is an excellent guide:

> Electronic storage of client files, like electronic communication, is generally acceptable, as long as lawyers take reasonable precautions to protect client information from further disclosure. Because one of the primary risks of electronic storage is the necessity of giving a third party access, lawyers should ensure that the third party promises to maintain the confidentiality of the information and to implement security measures that meet industry standards. *See, e.g.,* Maine Ethics Op 194 (2007) (firm may store client files electronically but must "take steps to ensure that the company providing… confidential data storage has a legally enforceable obligation to maintain the confidentiality"); Missouri Informal Ethics Op 2006-0092 (lawyer may use third party to store electronic backup of firm's files, but must receive assurances from third party that information will be kept secure "at a level that meets industry standards").
> Helen's article goes on to discuss electronic communications, metadata, third party disposal of client files, and other related topics.

So, what to do?

1. Be an active, informed consumer. Read and understand Dropbox's security policy.

2. Take special care with information that is particularly sensitive or subject to a confidentiality agreement. (*See Odds & Ends: Safeguarding Client Information in a Digital World*).
3. Remember the client is king: "… (I)f a client requests it, a lawyer may be required to avoid … a particular type of electronic communication notwithstanding expectations of privacy in the communication method."
4. Consider creating your own private volume on Dropbox with a private encryption key using TrueCrypt Volumes, a free open-source encryption software.
5. Maintain your perspective. Yes, Dropbox does cooperate with United States law enforcement when it receives "valid legal process," but they are not alone: "Google complies with valid legal process. It is Google's policy to notify users before turning over their data whenever possible and legally permissible." Also see, *Social Media and Law Enforcement: Who Gets What Data and When?* and *NSA has massive database of Americans' phone calls*.
6. Remain vigilant. Privacy policies change and so does technology.

Originally published June 14, 2011 at
http://oregonlawpracticemanagement.com/2011/06/14/dropbox-security-concerns/