ELECTRONIC COMMUNICATION CLAUSE IN AGREEMENT FOR LEGAL SERVICES

Is anyone putting a clause in their Agreement for Legal Services that says something to the effect that client is ok with attorney sending invoices, letters, etc., by email only; understands this includes confidential and privileged info; knows email not 100% secure even if attorney uses reasonable efforts; not going to be encrypted; willing to proceed anyway, blah blah blah?

Anyone expanding from there to address online chat, skype, VOIP, interactive websites, file sharing services, text messages, twitter DM, cell phones, etc.?

I'm trying to craft something for our agreement. We do a lot of work with tech startups and we're constantly being asked to communicate in the foregoing mediums. Just wondering what the collective thinks before we get too far into this.

This is what I use in my fee agreements:

Electronic Mail

In the course of our representation, we may have occasion to communicate with you or with others by electronic mail. Such communications will not be encrypted. Although interception of such communications by a third party would constitute a violation of federal law, we can offer no assurance that such interception will not occur. We will abide by any instructions you may give us concerning electronic mail communications; in the absence of such instructions, we will use our own judgment regarding the advisability of using such means of communication.

Walter D. James III, Texas

Keep an eye on what your state is doing from a regulatory standpoint. Massachusetts has adopted regulations that after several delays go into effect on 3/1/10. We will need to encrypt emails containing confidential information. The regulations set forth what is confidential with a chart, e.g., 1 piece of info from column A (name) with 1 piece of info from column B (SS# or account #), etc.

If we fail to encrypt, we face per se liability for identity fraud issues, treble damages and attorney's fees under the MA Consumer Protection Act.

Peter T. Clark, Massachusetts

I have been using this paragraph

You agree that we are authorized to communicate with you on cellular phones and e-mail notwithstanding the risk that unauthorized eavesdropping may occur during such communications, which may violate the confidential nature of our communications with you.

Mark J. Astarita, New York

DRAFT
Regarding attorney-client communications, it has become customary to use electronic mail transmitted via the internet, including the use of online commercial e-mail services that store information on their servers, for attorney-client communications, albeit upon the understanding that such use and storage may heighten the risk of inadvertent or unintended disclosures or other adverse consequences occurring. You have advised me that that you invite and prefer the use of such communications and services, and of cellular telephones, text messaging, and fax transmissions, because of their efficiency and convenience and that you are aware of and accept the risks of any adverse consequences, which could include the loss of attorney-client privilege and attorney work product confidentiality and other protections and the disclosure of confidential information.

Alan S. Goldberg, Virginia

I am curious as to why you include this paragraph. Have you had clients who did not want to communicate by email due to risk?
Why wouldn't you include this in communications that take place by mail (which can be opened by the Post Office) or that take place in an office (where staff could be listening in).

Carolyn Elefant, District of Columbia

Thank you for that response, Carolyn. This thread makes no sense to me.

Do people put a clause in their fee agreements that warns clients that the cleaning staff may see their file?

What about the computer guy you call when your printer isn't working?

What about FedEx?

Andrew Flusche, Virginia

My governing body and my insurer suggest similar language in our retainer agreements, that's why I do it.

I also have the computer dude and anyone else in the office sign an acknowledgement that they are aware of our privacy policy and that they agree that any information they access will be kept confidential. Again, because my governing body and my insurer recommend it.

Michele Allinotte

And while we're at it, why not warn them about telephone calls on land lines? If the phone company allows NSA to wiretap people's phones without a search warrant, it seems to me that an expectation of privacy for a land line phone call is at least as questionable as the privacy of a cell phone call.

Kevin W. Grierson, Virginia

Standards evolve.

Perhaps "we" (in the royal sense) accept the use of snail mail and landline telephones because the "technology" (although that seems like an odd word in the context of pen and paper) have been around for so long, and we expect that clients will understand the associated risks.

About 20 or 25 years ago, there was a case that held that a client speaking to his attorney using a cell phone waived the attorney-client privilege, because anyone with an inexpensive Radio Shack scanner could listen in on cell phone calls at that time. Not too long after that, the California Bar came out with an opinion that it was NOT reckless for attorneys to use cell phones (relying, in part, on the changed technology for cell phones, which now are more likely to use digital technology --which I understand is somewhat harder to intercept).

It may be that use of e-mail is now (or in the not-too-distant future will be) considered a "known" technology, with no need to warn clients about the possibility that it will be intercepted, misdirected, etc. Until that time, do you want to be the test case for the proposition that you should have informed your client about the risks of using those "newfangled" technologies?

Brian H. Cole, California

Land lines? LAND LINES?!!? Hah! Better talk about cell phone tracking data. See <http://blog.newsweek.com/blogs/declassified/archive/2010/02/10/can-the-fbi-secretly-track-your-cell-phone.aspx>, a nice blog post today by Newsweek's Michael Isikoff. (Tomorrow, EFF's Kevin Bankston will argue the case in the Third Circuit. He almost didn't make it there because of the weather, but he's there.)

James S. Tyre, California

The thing about cleaning staff is one of the issues with the Red Flag Rules (by the way, are we lawyers totally clear from that or is that still being fought out? I know the ABA was fighting and winning to keep lawyers from being subject to the Red Flag Rules but was there a final decision on that?). If we were subject to the Red Flag Rules, all of our confidential files would have to be under lock and key unless we were there to prevent anyone unauthorized from seeing them.

Naomi C. Fujimoto, Hawaii

As posted in another thread, The Florida Bar is considering a rule to mandate use of email for service of process without one word of security, encryption, etc.

Michael A. Gort, Florida

Look, some of this is a natural human tendency to overstate new or unknown risks and understate or underestimate old or known risks.

Back when cell phones first became popular there were some bar opinions to the effect that lawyers should not discuss confidential information on a cell phone, because there was a risk that someone with a scanner could intercept it. Now, granted, that could happen. But, first, deliberately intercepting a cell phone conversation is a violation of federal law and is a criminal offense. Second, scanners at the time had the cell phone frequencies 'blocked' so they were not supposed to be able to receive cell calls; although 1) there was a cottage industry in 'unblocking' them, and 2) under certain circumstances, a particular cell phone call would be 'mirrored' on a lower or higher frequency and could be picked up by a scanner inadvertently. But deliberate interception is a federal crime. Point is, is a cell phone 100% secure? No. But neither's a land line. First, it is RIDICULOUSLY easy to deliberately tap a land line; trust me, I

know whereof I speak on this. It's a violation of federal law, but from a technical viewpoint, it can be done very easily and cheaply; a lot more cheaply and easily than deliberately intercepting a cell phone call. Second, if a telephone lineman is working on phone lines, they may very well overhear a particular conversation; it would be inadvertent, but still it could happen. Likewise, once in a blue moon land lines get 'crossed' where a third party can hear one or both sides of someone else's conversation; it doesn't happen a lot, but it can happen. Additionally, hearing a conversation within the same house or building is as simple as picking up on an extension on the same line. Point is, land lines are not 100% secure, either; and given that most modern cell phones are digital, cell phone conversations are probably MORE secure than a land line at this point.

And as far as snail mail goes: deliberately intercepting someone else's mail is a federal crime. Does it happen? Sometimes, occasionally. And mail gets misdirected, sent to the wrong address, sometimes gets opened inadvertently; I get a bunch of envelopes in my mailbox and will open them and look; once in a blue moon I'll realize I'm not the addressee. Most of the time I catch it before I open it, but sometimes I don't. Doesn't happen a lot, but it does happen. Is Snail mail 100% secure? No. Likewise, I had client who sent me some documents a couple of months ago; it was correctly addressed to me at my business and was sent via Fedex or UPS. But, they delivered it to the wrong Ronald Jones; he got package, opened it up, realized that it wasn't him, called client up in Mass. and got my phone number, called me the next morning and ran it to me. No big deal. But it happens. Is this something people worry a lot about? No. Likewise, some lawyers keep files off site; typically in storage facility. Is that 100% secure? No. Likewise, cleaners, maintence types, whoever, may be able to peruse the files on a lawyers desk when they're not there. I don't know anyone who locks up every single piece of paper when they're not in the office.

The point is, we've got rules recognizing that inadvertent disclosure of confidential information is not an automatic violation of the rules of professional conduct. Can email be accessed by third parties, yeah, it can. But so can snail mail, so can a land line conversation, so can a cell phone conversation. Is it likely? No. Where do you draw the line on acceptable risk?

Ronald Jones, Florida

Lawyers are not subject to the Red Flag Rules and you can thank the ABA for that fact. When the FTC would not back down, ABA filed suit, got good opinion from the DC

Court. See, sometimes the ABA does good things for ALL attorneys, not just big firm, liberal ones.

Sharon Campbell, Texas

Peter

Could you point us to where we might find this chart?

John C. Thrasher, Vermont

I do not think it is an actual chart, unless someone made one from the law.

Something to consider is sending letters as a password protected PDF. It is relatively easy to make a PDF open only with a password, and you can give the client a password at the initial meeting to use.

Phil A. Taylor

---

quote from a Mass. FAQ of November 3, 2009:

OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION 10 Park Plaza Suite 5170, Boston MA 02116 (617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

Must I encrypt my email if it contains personal information? If it is not technically feasible to do so, then no. However, you should implement best practices by not sending unencrypted personal information in an email. There are alternative methods to communicate personal information other through email, such as establishing a secure website that requires safeguards such as a username and password to conduct transactions involving personal information...
I am an attorney. Do communications with clients already covered by the attorney-client privilege immunize me from complying with 201 CMR 17.00? If you own or license personal information, you must comply with 201 CMR 17.00 regardless of privileged or confidential communications. You must take steps outlined in 201 CMR 17.00 to protect the personal information taking into account your size, scope, resources, and need for security.
I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well? Yes. If you own or license personal information about a resident of the Commonwealth, you must comply with 201 CMR 17.00, even if you already comply with HIPAA.

Alan S. Goldberg

Snail mail most certainly is not completely secure. Back in the 60's (yes, I am that old), I was away at college and wrote letters to two girls I was seeing back home. Can you guess the outcome? Yep, put the letters in the wrong envelopes.

Nothing is completely secure.

Michael A. Gort

Data point interesting perhaps only to me: Cell phones today are probably more secure than land lines were 20 years ago. When I was in law school, on occasion I would be talking on the phone and hear, quite distinctly, another conversation on the line--no wiretapping necessary. Never had that happen with my cell phone.

Without delving into the specifics of privacy laws and privilege requirements (which I realize everyone needs to consider) I think the key in any communication with a client is a reasonable expectation of privacy. Conversations on a cell phone do carry some implicit risk because they are *mobile* phones, and it probably makes sense to take care that both parties are in locations where the conversation won't be overheard. All technological means of communication are hackable, but it strikes me that the biggest risk of inadvertent disclosure remains a lack of awareness of one's surroundings. I have heard people walking down the street with cell phones, or in elevators, having surprisingly private conversations within earshot of people they don't know--I think there's a tendency to shut the world out when you're chatting on the phone that isn't necessarily reciprocated by those around you.

Kevin W. Grierson

It was First American Title that had created the chart in a PowerPoint presentation for its agents. As Phil cites below, it is quite simple to look at 201 CMR 17.00 et seq. and realize the implications of this on a law practice. As an example, if you do any conveyancing and have the lender's 1003 application as part of your copies package, you're subject to the law. Here are the relevant provisions:

*

Personal information*, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a residentâ€™s financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Peter Clark