**A Contract Lawyer’s Field Notes on the Negotiation of Digital Privacy and Data Security Terms**

Eric Vieland[[1]](#footnote-0)

I’m the lead business attorney for a large organization whose online communications programs rely on dozens of hardware, software and communications services vendors. The organization also cares a great deal about digital privacy. So I spend a lot of time working with vendors, especially at the contract negotiation stage, trying to protect that privacy as much as possible. These notes summarize the major topics and challenges that I try to watch out for in that process.

1. **Keep your eyes open; digital privacy and data security can be at stake in a wide array of contracts**

While we may not have quite reached the point where digital privacy and data security issues are present in *every* contract for goods or services, we have come close enough that a careful lawyer will always go looking for them. That being said, there are categories of contracts in which those issues are sure to come up.

* + **Communications platforms and services**. Any product, service or facility that digitally connects people (or their devices) must address the privacy and security of the data being transmitted and/or stored.
	+ **ecommerce facilities**. Any service that facilitates digital financial transactions raises similar questions, but is likely to be under additional regulatory burdens.
	+ **Online advertising**. If you are placing a digital ad that is targeted to selected audiences, you probably want to know that the vendor got the targeting data in a palatable way. If anything happens when a targeted individual interacts with the ad in any way, then you probably also want to know what will happen to the data generated by that interaction.
	+ **Acquisition and sharing of contact lists and other personal information**. Similarly, if you are buying data about people, you probably want to know how it was sourced, and if you are selling or swapping data, you probably need to know how it will be handled.
	+ **Any connected product, device or service.** Systems that you are buying for the purpose of transmitting or storing data may be relatively easy to spot, but it can be harder to keep track of all the people and things that may be *connected to* those systems. The IT support person who comes to your client’s office to integrate some software; the app that lets your client receive internet traffic reports on her phone; the third-party service provider who will be plugged into your client’s website to support some special functionality. These situations (and many others) create data exposures that can be every bit as serious and difficult to address as those arising in more obvious contexts.
1. **Digital privacy comes in three basic flavors**

Digital privacy (as opposed to data security, discussed later) comes in three versions, corresponding to the three different categories of people who may be snooping: the vendor (and its agents and partners), government agencies (approaching the vendor openly for information), and everybody else, i.e. various types of hackers. Each of these categories requires its own line of analysis, and raises its own set of potential negotiating challenges.

* + **Snooping by the other party**
		- A promise by the other party to keep data “confidential” is probably not enough. You should specify, at a minimum, that this includes (i) using the data exclusively for the purposes set forth in the agreement, (ii) not disclosing the data to any other party, (iii) taking appropriate security measures to protect the data from inadvertent disclosure, and (iv) returning or destroying all copies, and all derivative versions, upon the termination of the agreement.
		- Some agreements, and some practitioners, use the language of “ownership” to stand in for some or all of these ideas. It may be important to specify that your client owns certain data, for other reasons, but that’s not a substitute for exacting the specific promises listed above.
		- Operational details of how the vendor does its job may make the promises listed above quite complicated. Maybe the vendor needs to use cookies, beacons or other such devices to manage traffic. Maybe the vendor needs to prepare and store derivative data, or even share depersonalized data across customer accounts, to make the product work. There are all sorts of ways to accommodate these things, but they can only be done correctly if you understand the operational details.
		- Data-related goods and services are rarely freestanding; many vendors have relationships with other businesses providing them with everything from staffing to software modules to data storage capacity. You need to know who all those parties are, make sure they are all willing and able to uphold the main vendor’s confidentiality promises, and—if possible—get the main vendor to guarantee their compliance. Yes, that guarantee ought to be implicit in the subcontracting arrangement, but in the context of nested tech providers there are a variety of reasons why you may need to force the issue.
	+ **Snooping by the government(s)**
		- Vendors may receive various types of requests, from government agencies, for information regarding your client or the end-users of your client’s communication platform. Compliance with those requests may be optional or mandatory, and the vendor may or may not have a legal right to tell your client about the requests, depending on the particular legal means chosen by the government in any instance.
		- The negotiating objective, therefore, is to limit the vendor’s discretionary cooperation with governmental inquiries, while recognizing the limits of that discretion. Typically, a vendor should promise (i) to notify your client of any request if and when it is legal to do so; (ii) if there has been such notice, to then cooperate in your client’s efforts to bar or limit any disclosure; and (iii) in any event, not to disclose anything unless legally compelled to do so, and then only to the extent required.
		- Although US federal law tends to be the dominant framework for this type of negotiation, when US clients are building US systems, foreign jurisdictions may be significant—not only if the system you are building will have international components, but even if the users are all domestic and you happen to be using a provider with overseas data centers or other operations. Some vendors give your client an option of having all data remain within the US, and this may be advantageous.
	+ **Snooping by hackers**
		- The vendor can’t typically be expected to offer an absolute guarantee against hacking, but your client should get reasonable assurances regarding the vendor’s security measures and ongoing diligence. The exact nature of those assurances will depend very much on the inherent strengths and weaknesses of the technology in play, so this is an example of an area in which good drafting must follow closely on good technological analysis.
		- If the vendor is expected to provide services for a long period, or if the vendor is to store critical data on its end, it may be appropriate for your client (probably through a separate security service provider) to be an active, ongoing participant in security diligence. Again, the specifics have to follow closely on technological analysis. But here the lawyer can play a more active role; ask the technologist whether it would be useful, and reasonable under the circumstances, to ask for measures such as periodic independent security audits of the vendor’s data facilities, or updates on changes in the vendor’s data architecture.
		- The vendor should be obliged to notify your client promptly of any security breaches (if not also to take specific remedial measures). The problem is that a “security breach” can actually be several different things, and some of those things may be very difficult for the vendor to identify under some circumstances. Will the vendor know if data has been accessed? How about an unsuccessful attempt to access data? How about the failure of some security measure, such that data was relatively exposed, even if no attempt was made to exploit that exposure? The vendor should agree to share whatever it does know in these regards, and your client should take in to account the problems that arise when this type of information is not available.
		- If you have negotiated any specific standards or warranties regarding security from third-party snooping, make sure there’s nothing lying around in another part of the agreement, such as the force majeure clause, that undercuts the vendor’s duties regarding actions by third parties.
1. **Privacy can be intertwined with other types of data security concerns**

In addition to the confidentiality of user information, digital privacy and data security may involve other related topics that should be negotiated in parallel. These other topics may be less likely to come up as critical in any given business arrangement, but when they do they may also require their own lanes of analysis and discussion.

* If anyone would be harmed by having data disappear, the vendor should show, and guarantee, robust features for protecting against loss of data. The potential injured party could be an end user who was depending on something being transmitted or stored, or, more usually, your client, who needs to know that the whole database will be available for the continuation of current activity or as a basis for subsequent activity.
* In some cases it may be critical to ensure against the corruption of data, for example in some situations where data files are being merged or superimposed. The vendor should be able to make appropriate representations regarding data integrity.
* It is sometimes critical to have very good means of authenticating the source of a message. The question of whether you need specific promises regarding authentication technology will tend to follow the question of whether you are facilitating monetary transactions, but there are other situations where a case of mistaken identity (by deceit or otherwise) could have bad consequences.
* Finally, if anybody is going to expect anonymity, that requires another line of discussion, since the protection of anonymity may require yet another set of tools, standards or data management strategies.
1. **Understand the limits of what you can provide your client by way of contractual recourse**

As difficult as it may be to understand which privacy and security measures your client needs, and which ones the vendor is willing and able to promise, it may be more difficult still to tie those promises to meaningful contractual remedies. Any or all of the following factors may contribute to that problem in any given negotiation.

* + It may be very difficult to put dollar values on injuries such as invasion of privacy or loss of data. The exception is that if the injury involves a security breach that is subject to state or federal rules on mandatory consumer notification, or other related remedies, it may be relatively easy to calculate the cost of the required responses. But even then, that calculation may be a poor measure of the damage done to individual end users or to your client’s enterprise.
	+ Vendors will routinely seek to exclude liability for indirect and consequential damages. But in this arena, virtually all damages are indirect or consequential, if those terms apply at all in the context of data handling. Be sure to carve back the specific forms of damage that matter.
	+ Vendors will routinely seek to cap liability at low levels, often pegged to the volume of fees paid by your client. No matter how correct you may be in saying that this is plainly inappropriate, and in pointing out that the relevant risks are controllable only by the vendor, be prepared to face some earnest shock and consternation at the suggestion that the vendor should stand behind its service. Be prepared to show your own shock and consternation that they’ve apparently never heard of commercial liability insurance.
	+ In some instances, it may be difficult to prove a breach. For example, if you can show that data escaped, but not exactly when and how it escaped, you may be unable to demonstrate that the escape constituted a breach of any particular promise by the vendor.
	+ Many of the provisions you negotiate will be for the benefit of other users (other than your client) exposing their personal information to the vendor. So you’ll need to pick a strategy for providing those users with direct recourse against the vendor, or for going after the vendor on their behalf, or of having your client make the users whole and then turn to the vendor for indemnification. And then having the contract support that strategy.
	+ If the vendor puts a form agreement on the table, any liability shifting provisions are likely to flow the other way, with (for example) your client assuming all responsibility for claims against the vendor by end users. While this may be appropriate in certain limited regards, such as a vendor’s responsibility for content provided by your client, it must not be allowed to extend to liability for the mishandling of user data by the vendor or its agents.
	+ You may also see mandatory mediation or arbitration clauses. These are inappropriate on several different levels for these types of contracts, but at a minimum note that your client may need to seek injunctive relief against certain data handling practices, and should preserve access to the courts at least with regard to that type of situation.
1. **You’ll often have to layer contracts together for multi-vendor systems**

Communications platforms and systems are typically composed of constellations of products and services, provided by different vendors. That arrangement creates some problems for the contracts lawyer.

* + In the multi-vendor context, contracts can only help create meaningful standards for data handling if you achieve two goals: (i) get all the vendors on board with materially the same set of standards, and (ii) define the vendors’ respective responsibilities so that you have a fighting chance of pinning any foreseeable data-related mishap on somebody in particular.
	+ Specific products and services are likely to have been included in the project because they offer unique capabilities. But those capabilities may be hard-wired to data handling techniques or standards that don’t fit the standards you are trying to build across the project. If you spot this early enough in the process, it may be possible to swap out a product or strategy; if not, then you may be stuck trying to limit the potential damage.
	+ There may be some vendors who don’t realize that their own products are themselves composite in nature. For example, a vendor may tell you in good faith that it doesn’t use any subcontractors. But when pressed to describe exactly where it stores high volumes of customer data, it may reveal that it uses an external cloud storage facility for that purpose. The vendor may simply think of that as a tool, but from your perspective, if that cloud provider is not part of the data security program for your client’s project, then you have not accomplished your goal. And don’t forget to ask how the vendor moves data to and from that cloud provider.
1. **A grab-bag of other problems**
	* Tech and data providers generally, and cloud services providers in particular, are enamored of “click-through” agreements that exist only as combinations of online pages linked to an “I accept” button. Increasingly, vendors think this is appropriate even for enterprise agreements, and (amazingly) to agreements with extensively negotiated terms. Large volumes of supporting documentation, including critical terms and conditions, may be incorporated through links. Many of the linked documents may recite that the vendor is free to amend them from time to time. While some vendors will help build a work-around if pushed to do so, you may occasionally find yourself challenged to demonstrate exactly what was agreed. A printed “contract proof,” including date-stamped screenshots of all the relevant online documentation, and hopefully including some sort of acknowledgement by the vendor that a contract was formed on that date, may be your last resort.
	* Clients who care a lot about privacy may also care a lot about free speech. Vendors who are cavalier about privacy may also be cavalier about free speech. So if you are negotiating on one topic, you may well also find yourself negotiating on the other. A cavalier attitude toward speech is likely to crop up in the vendor’s “acceptable use policy,” where the vendor may reserve the right to monitor communications and exclude users based on material being “offensive,” inappropriate” or any number of other criteria. Many vendors prohibit communications that “support terrorism,” without any guidance as to what that might mean. In all these regards, the vendor has a legitimate interest in having your client promise not to make or knowingly allow any *illegal* communications, but no legitimate interest in going any further. Deciding whether to fight on this topic is largely a judgment call separate from the rest of what is covered in this outline. But note that a vendor’s right to monitor or interfere in communications, buried in a provision on acceptable use, may undercut promises elsewhere regarding the vendor’s respect for the privacy of users.
	* If your client is building any sort of communication platform, or even just branding an iteration of a platform built by others, the client will probably want to write and post a privacy policy, and possibly other platform terms of use that affect how data is handled. One of your jobs is to make sure all the vendors providing pieces of that platform are willing and able to live within that posted policy. Another is to make sure your client understands that contact lists accumulated under a posted policy may effectively become permanently associated with that policy, i.e., once you’ve collected somebody’s name and email address under a very protective privacy policy, you may find it hard to use that contact data in novel and evolving contexts, at least without violating what amounts to a permanent set of promises to that individual.
	* Generations of data-related contracts have now been written using the term “Personally Identifying Information” to describe things like names, credit card numbers and social security numbers, and draw a protective fence around that particular type of data. That approach leaves other bits of information, not intuitively identifiable as belonging to any individual, free for the taking (e.g., an anonymized trail of a user moving through a series of web pages in a particular way, or a record that somebody looked at an ad for a certain product while sitting in a certain train station). While that PII/non-PII approach may once have been appropriate, it is no longer so. Modern data analytics can reverse-engineer personal identities, or at least specific device addresses, from data points that used to be safely treated as harmless. If you want to protect users, you now have to look at *all* the data being generated by, or harvested in connection with, their interactions with your client’s platform or service.
2. **Be prepared to adjust your expectations regarding your role as the attorney**
	* In other business contexts, lawyers can often do an adequate job with contract negotiations, operating on their own, even without a complete technical grasp of their client’s business and the vendor’s products; they can fudge over any lack of knowledge with contractual promises that are outcome-oriented, or otherwise broad enough to step over various operational details. Remedies that simply make the client whole if something doesn’t work are a favorite tool. But in the context of information systems, that strategy isn’t typically viable, for multiple reasons. Since these contracts are primarily about assembling products and protocols to create a secure environment, and provide remedies for failure only as a porous and distant second line of defense, a lawyer may do more harm than good if she relies on outcome-based negotiating strategies, and especially if she isn’t forthcoming about the limits of her expertise. Work with a technologist who can give you precise reads on where the vulnerabilities lie, where the vendor needs to agree to take specific, non-standard steps regarding data handling, and where system designs can safely be treated as secure. Ideally, that technologist is your client’s system designer.
	* While you may need to rely on a technologist to help you understand the design and performance limits of the vendor’s products, you can still take the lead on understanding the vendor’s business model. As in any negotiation, understanding the other side’s business model is the key to understanding where there is room for compromise. Information system vendors, from the very smallest to the very largest, often have particularly narrow and fixed business strategies; they’ve targeted a single way to move a product into a single niche, and that’s that. Make it a priority to know if that’s the situation you are facing, and what the negotiating implications are if so.
	* If you add up all the quirks discussed above, you see that a lawyer has to be prepared to surrender most of her normal role in business negotiation. We normally try to identify risks, eliminate them where we can, and shift ultimate responsibility for them to the other side where we can’t. But when your client is buying products that are inherently risky (and, typically, bundling them together), and especially when there’s no contractual remedy that will really make everybody whole if worse comes to worst, the lawyer may have to accept that the document on the table at the end of the negotiation process may not provide the types of protections she normally likes her clients to enjoy.
	* On the other hand, if the lawyer gets to the table early enough in the process, while the client (or the client’s system designer) is still considering products and strategies, the lawyer can play a critical role in identifying and assembling providers whose products and services are suitable to the client’s goals.
	* The lawyer also plays a critical role in advising the client as to the limitations of contracts in the information systems context. This often includes both lowering the client’s expectations, as to how much use a contract will be in the event of a data breach, and also raising those expectations, as to meaningful security, by focusing on specific practical measures the technologist can provide. Those may include things like client-controlled encryption environments, scans of vendors’ operating systems, and the segregation of data streams so that sensitive data flows only where necessary. The contract negotiation process can be an opportunity to help work out when and why these types of measures may be important.
	* Finally, the lawyer can play a critical role by providing clear and precise drafts, both of contract documents, and of notices and policies for end users. When it comes to digital privacy and data security risks, informed consent is a key concept, both for your client entering system agreements and for end users disclosing information to those systems. When you can’t reduce or shift risks, you can at least make sure that those assuming the risks have the best possible chance of understanding what they are doing.

\* \* \*

1. Eric Vieland is Corporate Counsel and Director of Risk Management for the American Civil Liberties Union. However, these notes reflect only his personal thoughts, and not any policy or activity of the ACLU. Of course these notes also may be incomplete or misleading as to any particular negotiation. They do not comprise legal advice and must not be taken as such. [↑](#footnote-ref-0)