ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003 **www.bobgellman.com**

The long and difficult road to a U.S. privacy law

These three blog posts originally appeared in the IAPP Daily in August 2018. The first is at https://iapp.org/news/a/the-long-and-difficult-road-to-a-u-s-privacy-law-part-1/, the second is at https://iapp.org/news/a/the-long-and-difficult-road-to-a-u-s-privacy-law-part-2/, and the third is at https://iapp.org/news/a/the-long-and-difficult-road-to-a-us-privacy-law-part-3/. This document with all three columns is at https://www.bobgellman.com/rg-docs/ RG-Blog-USPrivacyLaw-Aug2018.pdf.

A later post (October 2018) on an opt-in privacy law appears at https://iapp.org/news/a/one-way-to-solve-the-u-s-privacy-law-dilemma-an-opt-in-privacy-law/.

The long and difficult road to a U.S. privacy law: Part 1

A few years ago, the notion of a GDPR-like U.S. privacy law was a pipe dream. While many privacy advocates liked the idea of a broad privacy law, there was no support. Slowly, however, support for a broad U.S. law emerged, largely in response to pressure for simplifying international transfers of personal information. Still, that support was cautious, and no one put forward a specific, comprehensive, and realistic proposal. A vague and weak-kneed proposal took forever to emerge from the Obama administration, and it engendered no interest on Capitol Hill.

It's now a historical footnote.

Rumors suggest that some camps are developing specific proposals at this time, and a recent report revealed that the Department of Commerce is talking about privacy to some in the business community. It goes without saying, however, that it will be difficult to find common ground among the many interests at stake. It will be even more difficult to find a law that can pass here and that the EU will recognize as meeting the adequacy standard that would allow for the simple transfer of personal information from the EU to the U.S.

It is not my purpose here to pursue substantive issues that must be resolved to pass a useful general-purpose privacy bill. I want to focus on two little-recognized threshold barriers that exist. My views are informed in part by the seventeen years I spent in the House of Representatives as a staffer with responsibilities that included privacy.

The first barrier is overcoming the consequences of the so-called U.S. sectoral approach to privacy law. We already have privacy laws that cover various sectors of the economy, including credit reporting, federal agencies, schools, financial institutions, video rental, cable television, health, online children's privacy, and a few others. There is no space here to discuss the inconsistencies in these laws or the many activities with no privacy rules at all. Existing laws passed at different times, went through different congressional committees, and responded to

different types of pressure. It's hard to call these randomly passed laws an "approach," but I will set that issue aside.

What's notable about these laws is their differences.

Some laws are more privacy protective than others. Credit reporting privacy rules may be the best that we have. The federal health privacy law has a mixed bag of standards, but it only covers some of the health information in the U.S. The banking privacy law is so weak that it offers almost no meaningful privacy to consumers. The federal government privacy law is so old and outdated as to be laughable. Other laws are all over the place.

The problem is that with different existing statutory levels of privacy, any new generally applicable privacy law will necessarily raise privacy standards in some areas and lower them in others. It is certainly conceivable that a new law could meet the highest standard in any existing law, but the chances of that happening are nil.

So how will a new law reconcile new standards with existing rules?

Further, existing laws have different enforcement agencies and methods. Will a new law replace those agencies and methods? It is hard enough to find agreement on privacy standards. A new law that affects existing institutions by taking away existing authority will face major resistance from those institutions.

This bring us to the second problem. In the House of Representatives, at least six (and maybe more) legislative committees have jurisdiction over some existing privacy law or agency. Even committees with no laws under their belt today would likely claim an interest in a privacy bill. A general-purpose privacy bill that amends existing privacy laws will be referred to all the committees that reported out those laws. What generally happens to a bill that requires action by multiple committees? Nothing. It can be difficult or impossible to convince even three committees to act on the same proposal.

If six or more committees have jurisdiction over a privacy bill, there is only one hope. A broadly referred bill can reach the House floor only if the bill is a priority of the Speaker of the House. Only the Speaker can impose deadlines and discipline on so many committees. There are few precedents here, and only enormous political pressure or a personal interest from the Speaker can work. Even then, reconciling different views of the committees could prove impossible.

I do not know what will happen in the next election. However, I do not foresee any scenario that includes a powerful Speaker committed to privacy. This is likely true no matter who wins control of the House.

The Senate is a different world, and much happens there through negotiations and unanimous consent. A strongly committed Majority Leader can help, of course, but here too, it seems unlikely that the election will produce a Majority Leader with a privacy agenda. Regardless, jurisdictional fights between Senate committees stymied privacy legislation in the past, and it is hard to see how these fights would not recur.

There is a separate set of problems on the appropriations side of Capitol Hill. No one guards jurisdiction and power more jealously than the appropriations committees. If a new privacy bill transferred spending authority across existing appropriations subcommittee lines, that could well present another political and jurisdictional barrier to the bill.

I do not see any prospect in the immediate future for a general privacy law in the United States.

The barriers are large and complex, and I haven't even begun to address the substantive differences on the many complex policy matters must resolve. Nor have I addressed the massive lobbying campaign that a privacy bill would engender.

For now, the U.S. may be a captive of its so-called sectoral approach to privacy. We made our bed over the last 40 years or so, and we may have to lie in it for a long time.

The long and difficult road to a U.S. privacy law: Part 2

In the first part of this series, I discussed some of the political and structural problems that must be solved to pass any general U.S. data protection law. In this part, I discuss two of the most important substantive policy issues. They are the private right of action and federal preemption of state law. These may be the two hardest issues with the greatest gap between the business community on one side and consumer advocates on the other.

A PROA allows a consumer to sue a data controller (government or private sector) for violating their rights. A PROA may include class-action lawsuits on behalf of multiple consumers. From the perspective of consumers, class actions are crucial because the damages potentially available in a lawsuit brought by a single consumer are likely to be insufficient to support litigation. Private litigation is sometimes the only hope for enforcement because state and federal agencies do not have enough resources. Business sees class actions as an unwarranted expense that produces little gain for anyone other than trial lawyers, and there's no love lost between business and trial lawyers.

Compromise here is not impossible, but it will not be easy. The first compromise allows state attorneys general to enforce the federal privacy law. There's plenty of precedent here, and this is something likely to be part of even the narrowest business-supported bill. After all, state AGs are not all that aggressive. This is a step, but it won't be enough for consumers.

Another compromise is some form of enhanced enforcement by whatever federal agency or agencies have responsibility under the new law. People often point to the Federal Trade Commission as an effective privacy enforcer, but the FTC brings a relative handful of privacy cases. Still, better enforcement by an agency is not an impossibility. The Office for Civil Rights at the Department of Health and Human Services brings enforcement actions under HIPAA, the federal health privacy rules. In the recent past, OCR brought more privacy and security cases than the FTC by two orders of magnitude. Meaningful agency enforcement is not an impossibility.

Other compromises might allow some class actions but impose procedural or other barriers. A procedural barrier might require notice to the offender, with meaningful corrective action allowed as either an affirmative defense or in mitigation of damages. Limits on recoverable damages could also serve as a compromise. Some class-action lawyers told me that laws that allow the for recovery of gigantic damages (e.g., $100 per individual per violation per day) are barriers because the damages are so enormous that judges look for ways to find for defendants.

Some consumer groups look for and rely on class-action awards in the form of cy pres settlements of class actions where the damages per class member are too small to compensate individuals. There is much controversy here on all sides. Some question the efficacy of cy pres awards altogether, while consumer groups fight among themselves about who should get the money. Limits and procedures here might form a compromise.

Federal preemption of state privacy laws is perhaps the ultimate goal of the business community. Interest here increased lately because of the new California Consumer Privacy Act of 2018,

scheduled to take effect in 2020. Business not only worries about the California law but about the possibility that other states could pass similar laws with different requirements. Compliance with 50 state laws could easily be a nightmare. Business has an argument here. This is especially true in security, where complying with mildly variable state law requirements could be expensive or technically impossible.

On the other side, consumer advocates would surely call a weak federal privacy law with preemption a Privacy Prevention Act. Consumer groups feel just as strongly that states must be free to try new laws and provide protections better than federal law. Some federal laws began as a law passed by one state. The Drivers Privacy Protection Act is a good example. Further, consumers point to the federal health privacy rules as a precedent. HIPAA allows stronger state laws to remain in force. That has worked okay, but that's not to say that there are no problems.

Further, there's a new fly in the preemption ointment from net neutrality debates. A California proposal would enforce net neutrality indirectly by prohibiting the state from contracting with any service provider that does not meet designated standards. That "market"-based approach would be much harder for a federal law to preempt. It wouldn't work as neatly for privacy, but some major data companies could not afford to ignore large states.

What are possible compromises? First, federal preemption could be prospective only, covering new state laws but allowing existing laws to remain in force. The Fair Credit Reporting Act is an example.

Second, federal preemption could be limited. It is likely that all sides could agree on preemptive federal security standards. Other carve outs could be for enforcement or state records.

Third, federal preemption could be time limited. One way to do this is to preempt existing state laws but allow states to enact legislation starting five years after the effective date of the federal law. That would let the dust settle, identify gaps and shortcomings, and allow everyone to take up the fight later. Don't like five years? How about three or ten years?

This doesn't exhaust the realm of possible compromises, but neither of the two hardest issues is immune to compromise where both sides get something and give up something. For both sides, the losses will (and should) hurt.

Ultimately, the question is what do you get for compromising. There's something here that both sides want that could form the basis for an overall compromise on a broad federal privacy law. That something is the subject of the next part.

The long and difficult road to a U.S. privacy law: Part 3

This is the third and last in a series about the road to a general-purpose U.S. data protection law and the pitfalls on that road. The focus here is on areas of agreement between business and consumers. There are, in fact, some areas where the interests of both camps overlap.

Before moving there, we should acknowledge a major division in the business community.

Some American multinational companies see the need to move toward international (i.e., EU) data protection standards. These companies see one set of privacy rules that work everywhere as the least costly solution. Microsoft is an example. Others in the business community still wish that privacy would just go away. They would prefer a meaningless privacy law that gives consumers few rights, imposes few obligations on business, and totally preempts state laws. While a bit simplistic, for purpose of this discussion we can divide the business world into the privacy-willing and the privacy-unwilling camps.

The area of agreement between consumers and the privacy-willing business community should be clear. Both groups want to work toward a law that meets EU standards for adequacy. Consumer advocates recognize that broadly applicable requirements that implement EU data protection solutions will leave consumers better off than they are today. Privacy-willing businesses want a law recognized by the EU as adequate so that personal data can easily flow across international borders to the U.S.

There are, of course, a few barriers to reaching consensus. Let me count the ways. First, consumer advocates will want as much as they can get, while the privacy-willing businesses will want as little as they can get away with. There's still a lot of room in the middle here, even if we ignore the privacy-unwilling companies for a minute.

Second, it's not enough for all sides here to reach agreement on a privacy bill. In the end, it will be up to the EU to decide whether a law is "adequate" or not. The 2015 Schrems decision by the Court of Justice of the European Union narrowed the grounds for evaluating adequacy, holding that adequacy means equivalency. The Court also tossed out the weak-kneed, look-the-other-way, Safe Harbor agreement that papered over differences between the U.S. and the EU for about 15 years.

The Court's decision, fueled in part by the Snowden disclosures, started a process that led to a much more substantive set of standards for U.S. companies, the Privacy Shield. Even that remains controversial in Europe, and its ultimate prospects await another decision by the CJEU. Even if it survives, the Privacy Shield is cumbersome for willing participants. Other solutions to the data export problem like binding corporate rules and contracts are complex and expensive. A finding of adequacy would be much simpler for business.

Third, after all these years, some in the U.S. still think that they can "fool" Europe with a meaningless privacy law. There is no chance of that. The EU data protection establishment knows privacy backwards and forwards, and it will have no trouble evaluating any U.S. law. In my opinion, there is no case for the adequacy of any existing U.S. privacy law, except perhaps

the Fair Credit Reporting Act. We must move a long way to obtain an EU blessing, and we really won't know until after the law passes.

Fourth, one important EU standard is the requirement for an independent privacy agency. That will be hard. I addressed some of the difficulties in earlier parts of this series. No one should think that just giving more responsibility to the FTC will work. The agency would need an enormous boost in staff, authority, budget, and fortitude. It would also need jurisdiction over areas of the economy that have not been subject to the FTC at all (insurance, transportation, federal, state, and local governments, and more).

Personally, I've advocated for an independent privacy agency for more than thirty years. As a House staffer in the mid-1980s, I drafted the first modern privacy agency bill. Creating a new agency, however, would be just as challenging as enhancing the FTC or any other existing agency.

Fifth, no one should assume that the consumer advocacy community is monolithic. It is true that consumer groups mostly work together harmoniously today, much more than in the past. But when it comes to finding compromises, there are likely to be major disagreements. For example, one highly controversial part of the GDPR is the right to be forgotten. Civil liberties groups with strong concerns about the First Amendment will have different views on RTBF than some privacy groups. If internal differences are intense within the consumer (and business) community, progress will be slow or nonexistent.

Sixth, strong presidential and congressional leadership can be crucial in overcoming differences and enforcing discipline on negotiators. I don't think I need say much here about the absence of these qualities today.

Seventh, I observe that the U.S. and the EU often take a fundamentally different approach to making rules. The GDPR, like the Data Protection Directive before it, sets out broad policies. For example, the GDPR has a provision on data subject access rights that contains a few hundred words (336 actually), plus some nuance in a recital or two. A U.S. law could never be that simple. Every industry would lobby for its own flavor of limitation or exemption from access. The statute (or regulations) just on access would go on for page after page.

Finally, Europeans complained about intense lobbying by Americans as the GDPR moved through the process. If Congress seriously considered a privacy bill, every lobbyist in the U.S. would be active, and the EU lobbying on GDPR would look like child's play compared to what will happen here. Intense lobbying may be the final barrier to progress on privacy.

In the end, what are the real prospects for a broad U.S. privacy law?

It is apparent that there are many obstacles, substantive, procedural, and political. If everyone worked in good faith, it's conceivable that something acceptable could emerge in a few years. However, I don't think that there is enough consensus in the U.S. privacy world to have much hope right now. Maybe the dynamic will change as the EU moves to enforce the GDPR. Maybe not.

One way to solve the U.S. privacy law dilemma: An opt-in privacy law

Robert Gellman
October 12, 2018

The need for a comprehensive U.S. privacy law continues to grow, but the politics, procedures and policies of privacy are too complex to move legislation through the Congress. Here's a summary of why it's so hard, followed by a new idea.

The business community is split. Some multinationals might support a comprehensive privacy law that meets EU standards. Some domestic companies want a weak preemptive federal law that stops states like California from imposing meaningful privacy rules (the so-called Privacy Prevention Act). Other domestic companies that still hope that privacy will go away, and they want to do nothing.

The consumer, privacy, and civil rights advocacy communities share broadly similar goals for a privacy law, but it is far from clear whether their cohesiveness would continue when it comes time for compromise. On hard issues such as private rights of action and federal preemption, there could well be divergent positions among advocates. In any event, advocates don't have the oomph to push a federal bill through the process on their own.

Congress continues to show interest in privacy, but nothing useful emerges. Congress faces jurisdictional problems because many different committees have some jurisdiction over privacy legislation. Further, writing a new law when so many divergent sectoral privacy laws exist is a problem for which there is no existing solution.

An additional challenge is meeting EU standards. A weak privacy law that the EU will not recognize as "adequate" will not solve the problem for multinationals nor will it satisfy advocates. Yet an adequate law would attract strong opposition from parts of the business community. In the end, it may be hard to pass any law with any confidence that the EU will recognize it.

Just to complete this sketch of privacy, self-regulatory efforts in the U.S. are too weak, are too controlled by business, provide little more than the appearance of privacy, and don't meet international standards.

In other words, the privacy problem here in the U.S. is really hard to solve.

That is not news. Nothing can happen with a major compromise, and that's what I offer here. I don't have a fully comprehensive solution, but I suggest a way to address most of the major concerns of the multinational business community and the advocacy community. Those two interest groups might be enough to move a bill through the process, especially if other stakeholders have no basis for objection.

I propose an opt-in, federal privacy law for the commercial sector. The law will only apply to companies that affirmatively choose to comply with its terms. The model here comes from

arbitration. Laws define, support, and provide for the enforcement of arbitration agreements, but the parties to a contract usually decide whether they want to use arbitration. If they do not, then arbitration laws do not apply. The Privacy Shield, now available to solve some problems with U.S. companies that need to meet EU standards, is an opt-in program. Among its shortcomings is a failure to provide any protections for Americans.

With an opt-in privacy law, the data controller chooses to comply. There is no need for agreement from data subjects. Data subjects become the beneficiary of the decision along with the data controller.

What goes in the opt-in privacy law? The law has to address all elements of Fair Information Practices in a manner compatible with and similar to the GDPR. If the law isn't good enough to meet the EU adequacy standard, then companies that need to move personal data from the EU to the U.S. will not benefit. Meeting adequacy does not mean that the opt-in law must be identical to the GDPR, however.

The basic idea here is simple, but it won't be simple to draft a bill. For example, it is far from clear that the underfunded and underpowered FTC will meet EU standards for an independent privacy authority. Yet expanding the FTC's jurisdiction might attract broader opposition both inside and outside Congress. A new privacy agency has some attractiveness, but it will draw objections. Another hard issue is addressing the right-to-be-forgotten element of the GDPR given our strong First Amendment. There will be plenty of other challenges as well, but any approach to a privacy law will have similar obstacles.

One advantage of a strong law applicable only to the private sector is that all government issues disappear. Applying the same law to the government (federal, state, and local) would be a major political and substantive challenge. Another advantage is that jurisdictional conflicts within the Congress would diminish (but not disappear). A strong privacy law would likely be stronger than some existing federal privacy laws so conflicts would be minimal. That is not to say, however, that all conflicts with existing laws would go away. The federal health privacy rules present a particular challenge, as they apply to commercial and governmental entities.

For advocates, the proposal only accomplishes some of their objectives. There would be a strong privacy law meeting international standards. The main drawback is that many companies would not opt-in and would, for the most part, be left to set their own policies. Market pressure might be effective, at least to some degree. Companies such as data brokers that have few dealings with consumers would probably not opt-in. However, data brokers that do business with companies that opt-in to a privacy law might feel pressure from their customers to meet the new standards. A state could pass a law pushing its own agencies to do business with opt-in companies. Consumer pressure might induce many online companies and many merchants to opt-in. Regardless, however, an opt-in bill is still half a loaf, at best. That may be the best we can do right now.

For multinational businesses, an opt-in law deemed adequate by the EU would make international transfers simple. The businesses would no longer need to have contracts or adopt binding corporate rules, and there would be no need to meet the procedural requirements of the

Privacy Shield. These benefits would persuade large businesses to opt-in. Further, data processors who do business with opt-in companies would face pressure to opt-in themselves. Doing so would help processors preserve their existing business relationships and attract new business from other opt-in companies. If the opt-in law were sufficient robust, the stakes in a federal preemption fight would be reduced for those who opt in, and compromise on preemption might be easier to achieve.

In the end, the main device of the opt-in proposal is that it only applies to those who affirmatively choose to comply with the law. For those businesses that still want to do little about privacy, there would be no direct effect. They would be hard pressed to oppose a law that did not affect them, although they would probably oppose it anyway. Small businesses in particular could ignore the law as they see fit, and the argument that a privacy law is too costly for them disappears.

Is the opt-in proposal really practical? That is truly the question. It offers something to everyone, compels no one to do anything, provides some better privacy protections for consumers, acknowledges the robust international privacy movement, and generally puts the U.S. in a better position to address privacy standards already adopted by most of the rest of the world. The advantages of an opt-in privacy law would avoid some (but not all) of the difficulties that we face today.

An opt-in privacy law is not anyone’s perfect solution. It’s a compromise, not a panacea. But I submit that it is worthy of further debate and discussion.