Bloomberg BNA

Privacy and Security Law Report®

Privacy Enforcement

The traditional patchwork approach in the U.S. to privacy may have made sense in the context of U.S. politics and an evolving sense of privacy rights and interests over the past two decades, but recent developments over the past few years have highlighted a fundamental problem with this approach, the author writes.

Is the Sectoral Approach to Privacy Dead in the U.S.?

By Kirk J. Nahra

The European Union's general approach to privacy has always been straightforward. Privacy is a right, and the ''rules'' (whatever they may be) should apply to all data in all situations. It is (generally) a ''one size fits all'' approach, at least as a basic privacy baseline. The most recent developments to revise the general details of European privacy law, moving from the Data Protection Directive (95/46/EC) to the forthcoming General Data Protection Regulation, don't change this overall approach.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, where he represents companies in a broad range of industries in connection with privacy and data security laws and regulations across the U.S. and globally. Nahra, who is a member of the advisory board of Bloomberg BNA's Privacy & Security Law Report, can be reached at 202.719-7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.

The approach in the U.S., by contrast, is quite different. It is focused on two separate concepts—sectoral privacy laws and rules, for particular industries such as health care and financial services, and regulation of particular practices, such as telemarketing. This resulting hodgepodge (or the often used ''patchwork quilt'' description) can result in stronger or weaker privacy protections for certain information or in certain contexts than the EU approach, depending on the details of any particular law or regulation and the resulting gaps.

Although this approach may have made sense in the context of U.S. politics and an evolving sense of privacy rights and interests over the past two decades, recent developments over the past few years have highlighted a fundamental problem with this approach—our definition of appropriate ''sectors'' to regulate on privacy may no longer make sense, given how our industries are developing. At the same time, we have seen the explosion of ''big data'' analytics, coupled with new technologies and the Internet of things, which have broadened both the sources of new data about individuals and the ability to combine and analyze this data in ways never before thought possible. So, with this combination of developments, and the ongoing confusion about privacy rights and the competitive imbalances driven by different rules for similarly situated companies, is it time to declare a sectoral privacy approach dead?

Background

The volume of U.S. privacy laws and regulations is staggering (and is perhaps one reason why an entire profession of privacy professionals, led by the growing International Association of Privacy Professionals, has developed over the past decade). ''Financial institutions'' need to worry about the Gramm-Leach-Bliley Act

 ISSN 1538-3423

(GLBA). Health-care providers and health plans need to focus on the Health Insurance Portability and Accountability Act (HIPAA). Colleges and universities have the Family Educational Rights and Privacy Act. Video stores (do they still exist?) have the Video Privacy Protection Act. And the list goes on and on. This enormous and growing list causes confusion for both regulated entities and individuals, creating substantial compliance challenges without necessarily providing better privacy protection.

The Sector Challenge

As U.S. government entities began to evaluate privacy protections in commercial settings (primarily in the mid-1990s), at the dawn of the Internet era, sectoral privacy became the chosen approach. Some of this result was driven somewhat by accident, as new privacy laws and rules typically developed as an ''add-on'' to other kinds of substantive proposals. For example, the GLBA, one of the earliest ''sectoral'' privacy laws, was driven by the desire to remove certain Depression-era restrictions on potential business combinations between financial services companies and the insurance industry. It was a banking and insurance law, not a privacy law. However, as these larger financial services conglomerates were being authorized, Congress recognized a related concern about the privacy of consumer's financial data. While primarily focused on banks and insurers, the GLBA rules applied to financial institutions, a defined term that covers a broad range of entities (comprising at the time the financial services sector), ranging from insurers to banks to mutual funds, credit card companies and even tax preparers and auto dealers that offered car loans.

Developments related to health care web sites, personal health records, wearables and mobile applications has rendered the concept of a ''health-care industry,'' flawed from the beginning, largely untenable in terms of protecting personal health information.

HIPAA drew these sector lines even more starkly—leading many to be confused about the actual scope of the law. As discussed below, by focusing on a ''health care industry'' defined by activities unrelated to privacy, HIPAA only protects health information when it is held by or created by narrowly defined ''covered entities,'' such as health-care providers and health insurers. HIPAA doesn't protect health information collected in a wide variety of other contexts, including health care web sites, fitness devices, wearables, various health care mobile apps and a broad variety of health information held by retailers, pharmaceutical manufacturers and others.

How did we get to this counter-intuitive result? HIPAA was driven by two concepts, largely unconnected to privacy: the goal of ''portability'' of health insurance coverage, and the desire to create ''standard'' electronic health care transactions to provide increased efficiency for health-care services. Portability involved only a limited segment of the insurance industry. Standard transactions involved only certain kinds of health-care providers and health insurers. Privacy was essentially an afterthought in the HIPAA statute (with the statute itself containing no substantive privacy provisions), but the statute left the future regulators with a defined scope limited to ''covered entities,'' limited by the statute to certain (not all) health care providers and health plans (those entities involved in portability and/or standard transactions). So, even from the start of the HIPAA rules, the Department of Health and Human Services (tasked by Congress to develop rules when Congress couldn't create real privacy legislation) was forced to be creative to broaden privacy protections beyond those ''covered entities,'' by, for example, creating the idea of ''business associates'' and imposing contractual requirements on these covered entities when contracting with these vendors, and the rules governing ''group health plans,'' that attempted to draw lines between these regulated ''health plans'' and the employers that sponsored them. While these innovative concepts broadened privacy protections for individuals, they were stop-gap measures designed to supplement a limited grant of jurisdiction.

So, at the time of the original HIPAA rules, we knew that there were significant gaps in the HIPAA structure, but (1) there was no politically viable way to address them; and (2) we weren't all that worried about the gaps.

Now, through important developments related to health care web sites, personal health records, wearables and mobile applications, this concept of a ''health-care industry,'' flawed from the beginning, has now become largely untenable in terms of protecting personal information about health. Unless businesses gathering health information are closely linked to a covered entity, they aren't regulated by the HIPAA rules. Yet, a personal health record, typically obtained from a software company of some kind, can have every possible piece of health care information about an individual. Wearables track basic health care information. Mobile applications can track virtually anything in the health care space.[1] In today's structure, there is one set of rules if a health-care provider designs or provides a mobile app, and a totally different (and generally weaker) set of rules (if there are any rules at all) if the app developer builds the app and offers it directly to consumers.[2]

At the same time, even the idea of ''health information'' has become enormously confusing. For example, a recent report published on Bloomberg.com discussed

[1] A recent study indicated that ''health apps, like prescription drugs, come with side effects, it turns out. A new study has found that an astoundingly large number of health apps may be sharing users' medical information. . . . The bottom line: Most health apps are completely unregulated. If you don't want your information shared or the memory on your phone tampered with, be very careful about which apps you choose to download.'' *See* Eric Boodman, *Health apps aren't just collecting your info. They may be selling it, too*, STAT (March 8, 2016).

[2] *See* recent useful guidance from the Health and Human Services Office for Civil Rights, on when mobile applications may be subject to the HIPAA rules, and when they are not.

  PVLR ISSN 1538-3423

how physicians are obtaining a wide variety of behavioral indicators about their patients in order to monitor health risks. The story states that ''You may soon get a call from your doctor if you've let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores.''[3] Similarly, the New York Times reported on ''health plan prediction models'' that use consumer data obtained from data brokers, such as income, marital status, and number of cars owned, to predict emergency room use and urgent care needs.[4] So, when we see ''health businesses'' relying on data that isn't traditionally viewed as health care information and which is widely available outside of health care contexts and for a wide variety of non-health care usages, it's difficult to define and restrict what the concept of ''health information'' means. It also is clear that the HIPAA rules protect a broad variety of information when held by health-care providers or health insurers, such as your name and contact information, even if no one thinks of that information as ''health information.''

We also are seeing increasing concern about a variety of data gathering activities that clearly involve ''health,'' but for which there may be little or no current regulation of the collection and disclosure of this information (although there certainly are laws, such as the Fair Credit Reporting Act, that restrict some ways in which this data can be used to make decisions about individuals). Fortune Magazine recently reported on new employer data tracking activities, where ''Health care analytics companies can mine workers' medical claims, pharmacy claims, and search queries to figure out if an employee is trying to conceive or is already pregnant.[5] The Wall Street Journal reported that ''Employee wellness firms and insurers are working with companies to mine data about the prescription drugs workers use, how they shop and even whether they vote, to predict their individual health needs and recommend treatments.'' [6] These areas clearly are sensitive and risky, and employers should act cautiously in how they rely on this information for decision-making involving individuals, but the implications for sectoral privacy are clear: we are having real trouble defining the kinds of information and the types of entities that fit a sector and what that sector should be allowed to do (and prevented from doing) in connection with personal information.

The Telecommunications Debate

We are now seeing the HIPAA/Non-HIPAA debate begin to play out in connection with a new privacy-related agency, the Federal Communications Commission (FCC). The FCC has always had both a defined regulatory scope and, for many years, a specific set of privacy rules related to Consumer Proprietary Network Information (CPNI). For purposes largely unrelated to privacy, the FCC has acted to expand its overall jurisdiction in recent years.

Now, the Federal Communications Commission is proposing to move full force into the regulation of privacy for those entities within the scope of its activities.

The FCC originally regulated ''the communications industry,'' when that primarily meant television and radio companies, along with telephone companies, and has acted to expand its scope in recent decades as the communications industry has morphed with technological changes. Recently, through the ''net neutrality'' debate, the FCC also has taken action to regulate certain portions of the Internet. In addition, in the past year, the FCC also has begun to make headway into the regulation of data security activities.

Now, the FCC is proposing to move full force into the regulation of privacy for those entities within the scope of its activities. Regardless of your view of the substance of its proposals, it's clear that the FCC has the authority to regulate certain companies that have the perceived risks that the FCC is worried about, but has no authority to regulate other companies that present essentially the same risks (even with its broadened ''net neutrality'' jurisdiction). While it would be easy to take the position that ''something is better than nothing,'' this inability to effectively and consistently regulate certain practices because of an outdated definition of an industry sector is clearly a concern. The FCC may be acting to fill certain gaps in the regulatory structure (for example, for certain telecommunications companies perhaps outside the scope of the FCC's overall reach), but these actions likely will exacerbate the confusion and complexity of an approach that continues to focus on sectoral privacy regulation.

There is increasing concern that certain big data principles may weaken current privacy protections and create even larger gaps in the regulatory structure.

Therefore, given these increasing complexities in regulating the traditional ''sectors'' that have been the focus of U.S. privacy law, is it time to abandon this effort? It is clear that we cannot today meaningfully regulate a growing array of health information that is being collected and maintained outside of what HIPAA defines as the health-care industry. It is clear that ''the health-care industry'' is using a broad volume of ''non-health'' data in connection with its overall business activities and data analytics (and that this effort will continue to grow through new sources of data, often described as the ''Internet of things.'')

[3] *See* Shannon Pettypiece and Jordan Robertson, *Your Doctor Knows You're Killing Yourself. The Data Brokers Told Her*, Bloomberg Business (June 26, 2014).

[4] *See* Natasha Singer, *When a Health Plan Knows How You Shop*, N.Y. Times (June 28, 2014).

[5] *See* Valentina Zarya, *Employers Are Quietly Using Big Data to Track Employee Pregnancies*, Fortune (Feb. 17, 2016).

[6] *See* Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, Wall St. Journal (Feb. 17, 2016).

Now, with the communications industry, it is clear that the FCC's concerns about certain activities related to online behavior will be regulated (independent of the substance of this regulation) in a way that creates new gaps and competitive imbalances between companies that, while historically in separate industries, now are performing the same or similar functions, even though the defined jurisdiction for regulators has not kept pace with these real world changes.

Reporting on the recent FCC proposed rules, the New York Times put one of the issues starkly: ''The proposed regulations would put broadband providers under stronger privacy oversight than Internet companies like Google Inc. and Facebook Inc. Those companies are monitored by the Federal Trade Commission, whose ability to create specific privacy rules is limited.''[7] In the same New York Times article, the policy position of the potentially regulated entities was also quickly made clear. Quoting Bob Quinn, senior vice president for AT&T's federal regulatory affairs, ''Consumers expect and deserve consistent privacy protections for their online data, regardless of which company is collecting it and the technology used to collect it.''

How Big Data Complicates the Sectoral Debate

One of the driving factors for the increasing challenges to the sectoral approach derive from the development of ''big data'' and the related growth in the Internet of things, where enormous sources of new data, outside of traditional industry lines, are being developed. While big data is still new, there is increasing concern that certain big data principles may weaken current privacy protections and create even larger gaps in the regulatory structure. For example, in the context of this development, a recent White House report on Big Data stated that:

- A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education and the marketplace.
- The privacy frameworks that currently cover information now used in health may not be well suited to address these developments or facilitate the research that drives them.
- As big data enables ever more powerful discoveries, it will be important to re-visit how privacy is protected as information circulates among all the partners involved in care. Health care leaders have voiced the need for a broader trust framework to grant all health information, regardless of its source, some level of privacy protection.

FTC Commissioner Julie Brill already has become a leading voice on these issues. In a recent speech, she asked, ''then the question becomes, though, if we do have a law that protects health information but only in certain contexts, and then the same type of information or something very close to it is flowing outside of those silos that were created a long time ago, what does that mean? Are we comfortable with it? And should we be breaking down the legal silos to better protect that same health information when it is generated elsewhere.''[8]

Next Steps

So, the health care and communications debates present (generally) the same issue (and are simply two examples of this same dilemma): should privacy rights be based on the historic description of an industry sector, even if that sector no longer fits that historic definition, or should they be driven by the nature of the information itself, ''regardless of which company is collecting it and the technology used to collect it?'' It is clear that in the health care field, the rights for individuals are driven not by the information but by who is collecting it. The same issue already has arisen in the FCC debate, and likely will result in a set of rules that regulates part of the Internet but not all of it.

In the U.S., we can continue to add to the existing set of privacy laws and regulations, guaranteeing full employment on an ongoing basis to a wide variety of lawyers, consultants and privacy officers. We can regulate this kind of activity by one kind of entity one way, and a different kind of activity by a similar entity differently, ad infinitum. But, it is increasingly clear that this approach lacks any kind of consistent policy framework or cohesive set of protections, driven by either individual privacy interests or an appropriate balance between the benefits of commercial activity and the result protection of individual privacy. Instead, our privacy system is being driven by historic (and now often inaccurate) descriptions of an industry or, more precisely, by the scope of regulatory jurisdiction assigned to specific agencies for reasons unconnected to privacy protection.

We need to incorporate potential protections resulting from encryption and effective de-identification, to determine if there are ways to provide benefits from data without creating privacy risks.

It's time to look beyond this patchwork quilt of protections, to define the interests that individuals have in their personal data and the appropriate activities by business and commercial entities to utilize this data. Taking this step doesn't mean more or less protection for personal privacy—it is ''privacy neutral'' at its core. Instead, what this approach would push towards is a more coherent framework for privacy protection, one that is driven by specific goals and interests rather than historical accidents.

This approach will not be easy. While there may be a building consensus, particularly in the health care arena, that a new approach may be necessary, there is

[7] *See* Cecilia Kang, *F.C.C. Proposes Privacy Rules for Internet Providers*, N.Y. Times (March 10, 2016).

[8] *See* Brian Dolan, In-Depth: Consumer health and data privacy issues beyond HIPAA, MobiHealthNews (May 23, 2014).

  PVLR ISSN 1538-3423

no consensus whatsoever on the substance of this new approach. We have had little significant discussion about the benefits to individuals of certain uses of data, or the reasonable means of controlling how entities can use and disclose personal data. Obviously, any big picture resolution of this issue requires this discussion.

Putting aside political challenges (although these obviously cannot be ignored in the real world), there are options addressing the ''who should develop these principles'' ideas ranging from congressional legislation to broad rulemaking to industry self-regulation (including a composite approach including all of these approaches). On substance, we must grapple with the core issues presented by Fair Information Privacy Principles, to determine the role of individual notice and consent (if any), and the appropriate uses and disclosures for personal information for businesses (incorporating the concerns being raised by the White House Big Data report). We need to incorporate potential protections resulting from encryption and effective de-identification, to determine if there are ways to provide benefits from data without creating privacy risks.

There clearly is a long way to go. It is clear that there are ongoing and growing concerns about the sectoral approach, and the gaps and inconsistencies in privacy protection today. These concerns are not going away. There simply is too much interest in ''doing something'' about these issues for the discussion to stop. The debate will move forward, affected groups will make proposals, regulators will opine, and legislative hearings will be held. Industry groups may choose to develop guidelines or industry standards to forestall federal legislation. At a minimum, the policy-making ''noise'' on this issue should be substantial and ongoing for at least the next several years. It is clear that we're a long way from any agreement or consensus on defining any new rules to address these concerns, despite the growing consensus that there is a need to do something on these issues.

But, it's critical for privacy policymakers and affected individuals and businesses (which means virtually all of us) to understand that the current sectoral approach creates obvious gaps in privacy protections, results in significant inconsistencies among similarly situated businesses, and creates an environment where individuals have little ability to understand their rights and to evaluate how their information is being used, particularly by similarly situated entities who have different rules applied to them. If the sectoral approach to privacy isn't dead yet, maybe we should be taking action to kill it, sooner rather than later.