Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | January 2019

As we start off the new year, we are analyzing some of the key issues to be watching in 2019. We are expecting an enormous amount of activity on privacy and data security law, regulation, and enforcement this year. Joan Stewart reviews recent guidance on a lingering challenge under GDPR, the question of its territorial scope. Duane Pozza looks at recent developments related to Internet of Things payments. Our Election Law colleague, Lee Goodman, continues his discussion of First Amendment political privacy rights. And I review some of the most significant overall issues in privacy and security to watch in 2019. As always, please let me know if you have questions or comments on any of these topics, or if we can be of assistance in connection with any of these developments. Please let me know if you have thoughts on topics you would like us to address in future issues of *Privacy in Focus*. I can be reached at 202.719.7335 or **knahra@wileyrein.com**. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

ALSO IN THIS ISSUE

What to Watch for in Privacy and Security in 2019

Kirk J. Nahra

We can expect an enormous amount of activity for privacy and security professionals in 2019. While 2018 may have been as big a year as we have ever had for new privacy and security developments, 2019 may be just as important.

The Development of GDPR

While Europe has had significant privacy rules for more than 20 years, the EU General Data Protection Regulation (GDPR) caught everyone's attention to an unprecedented degree. Companies around the world raced the clock to get into compliance with the GDPR in May of 2018. We heard agitated reports (none of which should have been surprising) about the small percentage of companies that were in "full compliance" with the GDPR at this date – with these reports continuing today. Since that point (and continuing into 2019 and beyond), these companies (and the many others who were not aware of their obligations in May) will need to

continued on page 2

refine their GDPR compliance activities, paying close attention to ongoing official guidance, additional information about best practices and reported breaches or other problems. It is clear that GDPR compliance – like most privacy and security compliance – will be a long and winding road, and that there will be no obvious "end" to the compliance process. In fact, companies seeking to say "we're compliant and we are done" seem to be missing the main point.

The most critical issue to watch in 2019 will be enforcement. Some in the media have decried the lack of GDPR enforcement to date. That makes little sense to me – cases take time to investigate, and government regulators generally do not try to jump the gun on privacy investigations. At the same time, enforcement has started, and we can expect to see it ramp up significantly in 2019. I will be watching for two key things – what kinds of enforcement and how big are the penalties. On the first, we will see what the various privacy regulators care about. One note of caution, however – what happens "first" may not be what they care about the most; these may simply be the cases that are resolved the most quickly, either because the practices clearly are problematic or the target does not resist to the death. We already are aware of large-scale investigations into some of the world's largest tech companies – but what kind of enforcement will a "normal" company face?

The penalty issue may be more significant (although, again, this may reflect ease of negotiation rather than substance). The GDPR caught people's attention because of the potential for large fines – fines of up to 4% of an entity's "global annual turnover" (essentially revenue) for the preceding fiscal year, or 20,000,000 euros, whichever is higher. These are real numbers – if used. At the same time, even these enormous numbers may not matter much to some of the larger companies – raising the question of what kinds of penalties and enforcement might be "enough" to generate better behavior. If the regulators – who have substantial flexibility under the GDPR – start pushing the envelope on these amounts, particularly for "normal" companies, then all bets are off.

California's Privacy Law (and will there be others)

In June, California passed the California Consumer Privacy Act. It is a broad, general privacy law (scheduled to go into effect in 2020) that protects all California consumers and will apply to a broad range of companies, both in and out of California. It provides consumers with many rights (of varying levels of detail and complexity) concerning their personal data, with substantial compliance challenges for covered companies. It may be less prescriptive than the GDPR – but the rights may be more challenging to implement. The law also is in flux – it was written quickly, and has both obvious ambiguities (including such threshold questions as whether personal data is included in employment and professional contexts) and various ongoing points of debate. We will be watching how the language of the law evolves and is explained and whether the industry is able to water it down. We will watch whether the deadlines get extended, and how – when the law finally does go into effect – enforcement will proceed.

Perhaps more significantly, we also will be watching whether other states follow California's lead – resulting in both a broader range of privacy law and the possibility of

continued on page 3

continued from page 2

conflicts and tensions between the states. California's law is tough – and will create compliance challenges – but, much like the GDPR, companies likely will be able to navigate it. However, if we start getting other versions in other states – particularly with different provisions – then the compliance challenges magnify dramatically. California has an extensive history of privacy laws. Some of these laws exist in California and nowhere else. Some – even if they exist only in California (e.g., the law on privacy policies for websites) have a broader national impact. Some California laws (e.g., the SSN law) end up in many but not all states. The breach notification statute took more than a decade, but now exists in all states. Where will the newest California law land? It is highly unlikely that there will be 50 similar state laws – but it may only take three to five to tip the national debate in significant ways.

U.S. National Privacy Legislation

The GDPR and the new California law also have pushed privacy to the top of the national agenda. For the first time in recent memory, there is a significant debate about a national privacy law. Stakeholders are setting out their positions and principles, hearings are being held, and legislative language is being drafted. Preemption of state law, a private cause of action, and how to handle otherwise regulated sectors are on the core list of critical topics for debate (and there is no current consensus on any of these points). While there clearly is interest, on both sides of the political aisle, in some kind of national law, we are still a long way away from any meaningful consensus on the large or small points of such a law. But the activity on this potential national legislation during 2019 is likely to be frenetic.

Aside from these broad issues, I'm also watching carefully how existing laws will be factored into the national debate, particularly for the health care industry. We've always known that the Health Insurance Portability and Accountability Act (HIPAA) rules have meaningful gaps. At the same time – where it applies – HIPAA creates some important policy choices that have worked well for the health care industry and patients, and may prove useful as models for the national debate. Will the new law override HIPAA? Will it simply apply in addition to HIPAA? Or will heath care companies be carved out from the broader national law? The California law generally carves out HIPAA covered entities and business associates from coverage (although not without generating meaningful confusion). Many of the federal proposals are directed primarily at "unregulated" activities – and therefore also leave out HIPAA entities from new regulation. Will that approach continue? Does it make sense, given HIPAA's scope limits? If there is meaningful preemption of state law, will health care companies want to be subject to the new law, to benefit from preemption? There are lots of moving parts on this legislation, but the health care industry needs to make sure it is participating aggressively and thoughtfully in this ongoing debate.

The Federal Trade Commission

The Federal Trade Commission (FTC) is the default national privacy regulator, independent of specific industries. They have developed an aggressive approach to data security enforcement, based on more than 50 cases in recent years. At the same time, their authority on data security is under attack (including a highly confusing court result in 2018 as part of the extensive LabMD

continued on page 4

continued from page 3

proceedings), and FTC leadership is looking at focusing its enforcement only on situations where there is clear individual harm. In addition, the FTC has been less assertive in developing "privacy standards" – what is appropriate for consumers in connection with privacy – beyond deceptive practices. The FTC is under pressure from EU regulators to be active in enforcing Privacy Shield and privacy and data security in general. There are extensive debates that are ongoing about whether the FTC can be trusted to be the regulator if there is a national law. Other countries also look to the FTC for America's "position" on privacy issues. I'll be watching whether the FTC moves in new enforcement directions (which might reduce the need for a new privacy law), or whether it backs away on these issues or stays silent. I will be watching whether the recent challenges to data security enforcement make the FTC back away from its history. I will also be looking for whether the FTC has teeth in concluding some of its larger ingoing investigations – where both U.S. industry and international regulators will be watching whether the FTC can truly be the nation's privacy regulator.

The Next Big Security Breach or Privacy Scandal

We keep waiting for a privacy and security tipping point. Many of us have thought that the latest and greatest security breach (going back almost annually for a decade, whether it was Target, Sony, OPM, Anthem, Equifax, or other enormous breaches) would tip the vote towards national legislation on data security. We've been wrong each time – and now the debate is largely being driven by other events. We've seen recent tech company privacy scandals - almost too numerous to mention – shape the privacy debate. I will be watching whether the next problem, an enormous or risky security breach or a particularly juicy privacy scandal, will actually make any difference in how the federal government addresses privacy and data security issues. We all – consumers and companies alike – need to be paying close attention to this debate.

Hot Topics for the Health Care Industry

The core principles for privacy and data security in the health care industry are set out in the HIPAA Privacy and Security Rules. These rules – initially established early in the 21st century – have undergone one large modification (the HITECH statute and implementing regulations) and a small handful of otherwise modest changes.

I will be watching whether a current initiative – a "Request for Information" (RFI) from The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) – will result in significant modifications to the HIPAA Rules. The concept behind this RFI is two-fold. First there are various holdover issues still remaining (nine years later) from the HITECH statute – like the controversial HIPAA Accounting Rule. More broadly, the RFI looks at whether HIPAA creates impediments to "coordinated care" and other areas where a broader flow of patient information should be encouraged (think opioid crisis). While only the first step in what could be a lengthy regulatory process, we may see meaningful change to some of the core provisions of the HIPAA Rules (even in a context where it isn't clear any changes are necessary).

These efforts, however, also are highlighting some of the concerns with other aspects of health care privacy beyond HIPAA. For

continued on page 5

continued from page 4

example, many of the concerns in the RFI about data sharing for "coordinated care" and the opioid crisis actually seem rooted in other federal law (mainly the Part 2 rules on substance abuse information) and the enormous range of state laws that make data sharing harder in many contexts.

In addition, while the HIPAA Rules provide a baseline for the traditional health care industry, HIPAA has never been an overall health information privacy law. Limited by statute, the Privacy Rule applies only to "covered entities," mainly health care providers and health insurers. The RFI can't "fix" this limitation in any meaningful way. Over the past decade, we have seen an explosion of new kinds of health data being gathered, accessed, and analyzed by entities not subject to the HIPAA Rules, primarily (but not exclusively) in the direct-to-consumer context. The RFI cannot address these gaps – HHS cannot extend its regulations without congressional action outside of the set of covered entities – so currently there is a significant gap in regulatory obligations for this "non-HIPAA health data." For consumers, these gaps create privacy risks and confusion and potentially risks of discrimination and otherwise. For the entities gathering this highly sensitive data, there is an important challenge to act thoughtfully and responsibly even in the absence of firm governing principles. I will be watching how this issue evolves in 2019, and whether companies will appropriately safeguard this important information.

We also are seeing an enormous change in who is actually part of the health care industry. Some of this involves GDPR more than HIPAA – pharmaceutical companies, for example, have little direct concern under HIPAA (as they typically are not covered entities or business associates) but have meaningful compliance challenges under GDPR. In addition, one critical element of this "non-HIPAA" data involves the accelerating role of technology companies into the health care field. We are seeing aggressive moves into the health care industry – on almost a daily basis – by Amazon, Apple, and others, both to address perceived failures in the current industry and to make heath information more available to consumers through a variety of additional channels. Many of these consumer-driven activities will fall outside of the HIPAA rules. Some – particularly where technology companies may be moving directly into traditional health care industry activities – may subject these companies to new regulatory obligations. So, while the health care industry awaits the impact of these companies entering health care from a competitive direction, from a privacy perspective, we will need to see how consumer interests, loosely regulated environments, and health care disruption all combine to protect (or not protect) individual privacy interests – particularly for companies whose traditional use of personal data has not been driven by health care industry laws or ethics.

State Enforcement

We also are going to be watching whether the states become more involved in privacy and security enforcement in 2019. We are seeing some drop-offs in enforcement at the federal level (for example, the HHS Office for Civil Rights (OCR) generally has been quiet since the new Administration took office – but recently has shown more signs of life through a series of meaningful enforcement actions). Will the states step in to beef up the overall enforcement threat? We are

continued on page 6

continued from page 5

starting to see three important kinds of state enforcement from state attorneys general: (1) enforcement in the regulatory gaps (primarily but not exclusively in New York); (2) through concerted state activity to take action under the HIPAA Rules (where state AGs have formal enforcement authority in addition to OCR); and (3) concerted action on broad national privacy issues (e.g., the recent national settlement involving Uber). Much like the FTC, the state AGs have authority to pursue a broad range of privacy and security cases – but they have not historically done much with this authority. We are seeing some modest changes in this area – but it will be important to see if this growth in state enforcement continues.

Conclusions

As a privacy lawyer, my need to learn and participate in new activities grows every day. For companies – with an ever-growing range of data available and new opportunities for analytics and other data crunching activities – the challenges for privacy and security are now a core corporate priority across virtually every industry. For consumers, the confusion and complexity has never been greater. We are seeing the privacy debate grow louder on a regular basis – but we are nowhere closer to any reasonable "solution." I expect 2019 to be a year of discussion, debate, enforcement, risks, and other challenges. I think we will make progress toward a U.S. national law – but we are unlikely to see that debate reach any meaningful conclusions. At the same time, through the growing Internet of Things and other broad uses of data, an increasing range of companies now need to be paying close attention to these issues – many of them companies that have not historically had large amounts of personal data, including car companies, refrigerator and thermostat makers, toy companies, and the growing number of companies that make personal data use a part of their business model. This leaves companies with an increased need to think about privacy and security strategically, and to learn as much as they can about both their own data needs and the evolving regulatory and enforcement regimes related to the overall use and disclosure of personal information. ■

For additional information on such future possibilities, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

New Issues Raised By Internet Of Things Payments

By Duane C. Pozza

The internet of things is a promising platform for all sorts of consumer services — and one coming fast is IoT payments. This holiday season, for example, Amazon reported huge sales of internet-connected home devices and a jump in consumers ordering products using those same kinds of devices. The development of IoT payments will bring great benefits to consumers, but just as with the move to mobile over the last decade, companies need to carefully think through implementation. How do existing laws apply to transactions executed using a wide range of connected devices? How should companies proactively address the attendant risks?

What Are IoT Payments?

IoT payments come in a range of forms. A person can order a product online through a smart home assistant, or set up a refrigerator to manage and order groceries. A consumer can use a wearable device like a watch to make an in-store contactless payment or even an in-app payment. Connected cars can search for nearby gas stations and pay automatically. These kinds of use cases will only grow as consumers increasingly rely on and become more comfortable with IoT devices — just as consumers shifted their habits from desktop computers to mobile devices over the last decade.

What New Issues Do They Raise?

Plenty of consumer laws and regulations apply to payments, and a key challenge is figuring out how they fit when payments are integrated into IoT devices — particularly given that these devices may have small or no screens, or rely on voice interaction to operate. Here are a few issues to watch:

Getting Consent for Transactions

In the world of payments, eliminating user friction is an important goal. One of the advantages of IoT payments is that consumers don't need to re-enter payment credentials for every purchase. At the same time, consumers must provide some sort of authorization for the transaction. For example, a refrigerator may be smart enough to order groceries on its own, but its owner won't want it to get ahead of what he or she authorized. And both the fridge operator and owner may be wary that kids in the household will use the connected functionality to stock the fridge with their favorite treats.

The Federal Trade Commission has brought multiple actions against companies that it alleged had failed to take sufficient steps to gain authorization for transactions, under Section 5 of the FTC Act. In resolving those actions, the FTC has generally permitted companies to obtain advance consent for transactions, while requiring that the scope of that consent be clearly and conspicuously disclosed to consumers in connection with obtaining authorization. In the context of cases in which kids were alleged to have made unauthorized purchases, it has also required that the disclosures and consent mechanism be reasonably calculated to ensure that the person providing consent is the account holder. So, for example, in obtaining consent for future grocery purchases, a company will want to look closely at how it informs consumers what they're authorizing when they set up instructions for future orders. And companies will want to think through whether kids or other unauthorized individuals are likely to incur unauthorized charges on IoT devices —

continued on page 8

continued from page 7

particularly those not under normal parental supervision — and what kinds of reasonable measures to take to verify an adult is behind the purchases.

For recurring purchases using IoT devices, an additional issue is compliance with the Restore Online Shoppers' Confidence Act, which prohibits companies from charging consumers for goods or services over the internet through a negative option feature (e.g., automatic renewal), without (1) clearly and conspicuously disclosing all material terms of the transaction before obtaining billing information; (2) obtaining the consumer's express informed consent before charging the consumer; and (3) providing "simple mechanisms" for a consumer to stop recurring charges. The FTC has not yet applied ROSCA in the IoT context, but the FTC has brought an action against an app developer for failing to disclose, before collecting billing information, the "simple mechanism" for stopping recurring charges, alleging that linking to a terms of service containing this information was insufficient. Communicating that kind of information can be challenging depending on a device's user interfaces.

Clarifying Payment Mechanisms and Dispute Rights

Different payment options — credit, debit and prepaid — have different statutory and regulatory protections if something goes wrong. (Prepaid account regulations will change when the CFPB's final prepaid rule goes into effect in early 2019). For example, liability for unauthorized use of a credit card is capped at $50 under Regulation Z, implementing the Truth in Lending Act. If a payment is linked to a debit card, however, a consumer must report the transaction within 2 business days to cap liability at $50, and could face greater costs if reporting is further delayed, under Regulation E (implementing the Electronic Fund Transfer Act).

In the context of mobile payments, the FTC has flagged that consumers could potentially be confused about which funding source a consumer is using to make a payment and what liability protections they have. The FTC has not yet brought any enforcement actions based on this kind of confusion, which would require proof that consumers had been misled about a material fact of a transaction. But IoT payments may provide further challenges in this area. In a mobile payment, a consumer may see a screen that shows the card or account being used, while IoT payments may not involve a screen at all. If an IoT account — like many mobile accounts — is linked to multiple funding options, companies will want to think carefully about how to communicate any choices or defaults to consumers.

Communicating Privacy Choices

Both the federal government and states are actively evaluating whether and how to give consumers more control over use and disclosure of their personal data, including data that is collected in the course of payment transactions. This is a potential challenge for companies involved in IoT payments. In an online or mobile transaction, consumers can review privacy policies or disclosures, and make decisions about data use, on the same device — but that option may not be realistic with an IoT device.

In the case of financial or transaction data, there are guideposts in existing law. Under Section 5 of the FTC Act and similar state laws, privacy representations must be

continued on page 9

continued from page 8

nondeceptive. The FTC has brought many cases where consumers thought they were keeping some information private, but in fact the data was shared — including one recent case involving transaction history on a mobile app. And a company involved in IoT payments will want to assess whether it qualifies as a "financial institution" under the Gramm-Leach-Bliley Act and is subject to the FTC's privacy rule. The FTC recently alleged, for example, that the operator of a peer-to-peer payment application qualified as a financial institution and that it violated the privacy rule by failing to provide a clear and conspicuous initial privacy notice, as required by the rule.

Over the next year, Congress, states and agencies like the FTC, the National Institute of Standards and Technology and National Telecommunications and Information Administration may all weigh in with further regulations or guidelines on consumer privacy that could impact the design and implementation of privacy choices in IoT transactions.

Security

Cybersecurity remains a top concern for IoT market participants, and payments add another layer of complexity. For one, using payment card information triggers the payment card industry's data security standard, or PCI DSS, requiring certain measures to protect cardholder data, including securing the entire cardholder data environment. Depending on the network architecture, that can include other internet-linked devices. Companies that fail to comply with PCI DSS requirements can face significant fines. Additionally, the risk of a breach includes payment card compromise or fraud that can result in even more financial exposure.

The FTC and, increasingly, states have also brought actions based on breaches — or even just vulnerabilities. For example, the New York attorney general recently announced a settlement with five companies whose mobile apps, it alleged, failed to properly authenticate SSL/TLS certificates, leaving them vulnerable to a so-called "man-in-the-middle" attack to obtain consumer credit card information. And the attorney general specifically noted that the office itself had tested the mobile apps to uncover security vulnerabilities, rather than responding to a complaint about stolen data. Industry participants have focused on cybersecurity issues in IoT in recent years, and will need to take account of device payment capabilities as well.

Conclusion

All signs point to payments growing in the IoT space in 2019 and beyond — a development that should bring benefits for consumers. As the numbers of IoT devices grow and their functionality expands into payments, industry participants will confront issues like the ones noted above in building out their products and services. Now is the time for companies to think through compliance as they scale up — to safeguard their own interests and benefit their customers. ■

For more information, please contact:
Duane C. Pozza
202.719.4533
dpozza@wileyrein.com

This article was first published by *Law360* on January 4, 2019 and is available **here**.

New Guidance on the Territorial Scope of the GDPR

By Joan Stewart

The General Data Protection Regulation (GDPR) is a sweeping privacy regulation notable for its broad territorial reach that pulled many companies and organizations with no physical connection to the European Union (EU) under its umbrella. As with previous EU privacy regulations, the GDPR applies to companies that are established in the EU. However, unlike previous regulations, the GDPR also applies to companies with no presence in the EU that offer goods or services to individuals in the EU. This second element – the targeting of individuals in the EU – has caused significant confusion and angst as companies worldwide debated whether merely having a website that was accessible from the EU required that they comply with its onerous obligations.

Recently, the European Data Protection Board (EDPB) – the organization responsible for the consistent application of the GDPR across member states – issued guidance that clarified in part when a company without an EU presence could become subject to the GDPR. The EDPB's guidance, issued in late November 2018, provides context and real-world examples to help companies assess their contact with the EU to determine if their operations are subject to the GDPR.

The EDPB guidance confirms that there must be some intention to offer a good or service to an individual in the EU. Thus, the first step for non-EU based companies is to determine if they are in fact offering a good or service. For example, the EDPB notes that the processing of HR data is not the offering of a good or service.

If your company is offering a good or service, the next step is to determine whether the good or service is actively directed to an individual in the EU. As clarified by the EDPB, this means that there must be an intention to direct the good or service to an individual in the EU. For example, a U.S.-based company that offers an app that is specific to a service in the EU, such as an interactive map of London, Paris, or Berlin, would be subject to the GDPR. But a U.S.-based company that offers a U.S. news app that happens to be downloaded and consulted while an individual is traveling in the EU would not be subject to the regulation because there is no intention to target an individual in the EU.

Likewise, for a company that has an online presence, the EDPB confirms that the mere fact that a website can be accessed from the EU or an individual in the EU purchases a product from the website would not necessarily subject the website operator to the GDPR's requirements. Rather, there needs to be a clear intention to sell the good or service to an individual in the EU. Examples of factors that demonstrate this intention are: offering payment options in EU currencies, offering information in the language of a member state, using a search engine operator to direct EU traffic toward the website, the international nature of the service (e.g., tourist services), a dedicated address or phone number in the EU, use of a top-level domain from the EU, or testimonials from EU clientele.

While the EDPB guidance does not narrow the territorial scope of the GDPR, it provides some welcome context to help companies with no EU presence assess if their online operations will trigger the GDPR. ■

For more information, please contact:
Joan Stewart
202.719.7438
jstewart@wileyrein.com

The First Amendment Right to Political Privacy

Chapter 4—NAACP v. Alabama

By Lee E. Goodman

The first three chapters of this series traced the jurisprudential evolution of the First Amendment right to political privacy – the individual right to keep political beliefs and associations private against government inquisition. Chapter 1 considered the unsuccessful attempts by the KKK, in the 1920s, and by American communists, in the 1940s, to preserve the anonymity of their fellow travelers. Chapter 2 covered a successful legal effort by an American conservative to preserve the anonymity of like-minded book purchasers in 1953. And Chapter 3 covered a successful legal challenge by a Marxist economist to keep secret the names of fellow Progressive Party partisans in 1957. The First Amendment's protection for political privacy started as a dissenting idea but gradually made its way into concurring opinions and eventually majority opinions. But it had yet to predicate the holding of a Supreme Court majority. That finally occurred in 1958, when a consensus of Justices held the First Amendment prohibited the State of Alabama from forcing the National Association for the Advancement of Colored People (NAACP) to turn over to the State its list of members and donors. The Supreme Court's unanimous First Amendment ruling in *NAACP v. Alabama* is the subject of this chapter.

Background – Alabama Justice

The NAACP was founded in 1909 and incorporated in 1911 in New York for the purpose of advocating for racial justice and equal rights through various political, social and legal means.

In the 1940s and 1950s, as the national civil rights movement intensified at state and local levels, the NAACP was in the forefront of organizing civil rights protests, advocating civil rights legislation and policy changes, and litigating civil rights challenges to discriminatory laws, especially in southern states. These efforts were increasingly successful, as evidenced by the Supreme Court's decision in *Brown v. Board of Education of Topeka, Kansas* in 1954.[1]

The NAACP's legal and other political efforts to change the status quo were not popular among white elected officials. This was true in Alabama where, among other activities, beginning in 1955, the local NAACP chapter instigated the civil disobedience of Rosa Parks. Rosa Parks was the Secretary of the Alabama Chapter of the NAACP. She was drafted to take a "white seat" on a bus in order to provoke a police response. Thereafter, the NAACP helped organize the year-long bus boycott under the hand-picked leadership of the young local Reverend Martin Luther King, Jr. The NAACP's Legal Defense Fund then funded the successful challenge to Montgomery's segregated bus system in the courts, effectively ending the boycott.[2] Such inconvenient political activism in Alabama by a national organization from New York must have gotten the Alabama political establishment to thinking about ways to impede its continuation, much the same way other southern states were doing, by investigating and exposing members and financial supporters,[3] and much the same way that the House Un-American Activities Committee sought to root out and discourage American communists (see Chapter 1) and the Buchanan Committee sought to disrupt

continued on page 12

Chapter 4—NAACP v. Alabama

continued from page 11

the free market advocacy of the Committee on Constitutional Government (see Chapter 2).

Since 1918, a state chapter of the NAACP had operated in Alabama as an unincorporated association. Members of the Alabama chapter constituted membership in the national organization. In 1951, the NAACP, headquartered in New York, had opened a regional office in Alabama, employing three people. But the NAACP had not complied with Alabama's state law requiring foreign corporations doing business inside the state to register with the Secretary of State and designate a place of business and agent to receive legal service.

In 1956, while the bus boycott was ongoing, the Attorney General of Alabama, John Patterson, filed a civil action in state court in Montgomery to enjoin the NAACP from conducting further activities within Alabama and effectively "to oust it from" Alabama.[4] The Attorney General pointed to numerous activities the NAACP had engaged in within Alabama: It had opened and operated a regional office, solicited financial contributions from citizens of Alabama, recruited members, organized state affiliate organizations, funded lawsuits in the state, and supported the bus boycott.[5] The state court issued an *ex parte* restraining order prohibiting the NAACP from engaging in further activities and forbidding the organization from taking any steps to qualify to do business.[6] The NAACP demurred, arguing that the statute did not apply to its political activities and, in any event, the objective of the Attorney General's suit "would violate rights to freedom of speech and assembly guaranteed under the Fourteenth Amendment to the Constitution of the United States."[7]

Before a hearing could be held, the Attorney General moved for a court order requiring the NAACP to produce voluminous organizational business records as well as "records containing the names and addresses of all Alabama 'members' and 'agents' of the Association."[8] The Attorney General argued these records were necessary to establish that the organization was indeed doing business in the state.[9] Over the NAACP's objections, the state court ordered the NAACP to produce the majority of the records sought, "including the membership lists."[10]

By the time of a hearing, the NAACP had offered to comply with the registration requirements for out of state enterprises doing business in Alabama. However, it did not comply with the state court's discovery production order. The state court ruled that the NAACP was in civil contempt and fined the organization $10,000. The state court's order provided that the fine would be forgiven if the organization complied within five days or increased to $100,000 if it failed to comply.[11]

Within five days, the NAACP produced virtually all of the records required under the order – except for its membership lists. The NAACP asserted that Alabama could not compel disclosure of its membership lists under the First and Fourteenth Amendments to the Constitution. The NAACP declined to produce its list of Alabama members because, in its view, the state court's discovery order "*per se* constituted an abridgement of its rights and those of its

continued on page 13

continued from page 12

members to freedom of association and free speech, and because of its belief that to comply with the order would subject [the NAACP] to destruction and its members to reprisals and harassment, thereby effectively depriving [the NAACP] and its members of the right to the exercise of freedom of association and free speech."[12]

In support of this contention, the NAACP submitted to the state court "affidavits showing that members of the N.A.A.C.P. in nearby counties had been subjected to reprisals when identified as signers of a school desegregation petition, and a showing of evidence of hostility to the purposes and aims of the organization in Alabama, and evidence that groups in the state were organized for the express purpose of ruthlessly suppressing [the NAACP's] program and policy."[13]

On this basis, the NAACP moved the state court to modify or vacate the contempt ruling or to stay its enforcement pending appellate review.[14] The state court denied the motion.[15] The Alabama Supreme Court denied certiorari on two appeals by the NAACP.[16]

Moreover, the state courts put the NAACP into a catch-22. Until it purged itself of contempt by producing the membership list, the NAACP could not contest the underlying civil action on the registration requirement or register itself. This effectively banned the NAACP from conducting any activity in the State of Alabama. And all of this was happening in 1956 while the NAACP was funding litigation before the Alabama federal court over bus segregation and the bus boycott was ongoing.

The NAACP appealed to the U.S. Supreme Court, and the Court granted certiorari in 1957.[17]

The NAACP's Arguments

The NAACP asserted before the Supreme Court, as it had argued before the state court, that disclosure and exposure of its members and financial supporters would violate the First and Fourteenth Amendments because of "bitter opposition" to its political objectives at all levels of government and in society at large in Alabama.[18] "Threatened and actual loss of employment and other forms of economic reprisals have accompanied legislation intended to punish financially those persons who advocate orderly compliance with the law as well as those who advocate equal rights for all," as well as violence, the NAACP asserted.[19] "Negroes who seek to secure their constitutional rights do so at peril of intimidation, vilification, economic reprisals, and physical harm."[20]

In this environment, the NAACP argued that "[d]isclosure of petitioner's members or threat of such disclosure will necessarily tend to curb the activities of petitioner and its members and weaken the strength and effectiveness of the organization in pursuit of its objectives in Alabama."[21]

In June of 1957, the Supreme Court had ruled in favor of efforts by American communists to resist government subpoenas in two Red Monday cases, *Sweezy v. New Hampshire*[22] and *Watkins v. United States*.[23] Both decisions figured prominently in the NAACP's brief, which cited *Sweezy* 12 times

continued on page 14

continued from page 13

and *Watkins* 10 times.[24] The NAACP also cited *United States v. Rumely*,[25] another successful defense against government subpoena, 7 times. Citation to these Court decisions, and copious quotation of Justice Frankfurter's concurrence in *Sweezy*, formed a refrain throughout the NAACP's cogent briefs.

The NAACP also pressed a broader argument in its reply brief – that the First Amendment protects "anonymous speech."[26] The NAACP invoked the history of anonymous publications in England, colonial America, and the early days of the United States, as well as the right to a secret ballot, and Justice Frankfurter's concurrence in *Sweezy*. "Anonymity, secrecy, privacy, however it may be called, thus has a special value in a democratic society," the NAACP argued.[27]

The State of Alabama's Arguments

In response, Alabama pressed principally three arguments. First, it argued that the NAACP did not have standing to assert the First Amendment rights of its individual members.[28] Second, it argued that any burden on the NAACP's associational rights would be the result of private opprobrium, not official state action.[29] And finally, the state argued that it had an overriding need for the membership lists in order to establish, in state court, that the NAACP was indeed conducting activities within Alabama in violation of the state corporate registration statute.[30] The existence of dues-paying members in Alabama would prove activity in the state.

Significantly, Alabama did *not* argue against First Amendment protection for private association. And it conceded that the NAACP, as a corporation, could assert its own First Amendment rights, but not its members.

The Supreme Court's Unanimous Ruling

In a unanimous decision written by Justice John Harlan, and without any concurring or dissenting opinions, the Court held in favor of NAACP.

The Court first held that the NAACP had standing to assert the protection of the First Amendment "because it and its members are in every practical sense identical."[31] In drawing this conclusion, the Court pointed to the "reasonable likelihood that the Association itself through diminished financial support and membership may be adversely affected if production is compelled…."[32]

On the First Amendment right asserted, the Court analogized the exposure of NAACP members to the government forcing members of certain faiths and political parties to wear arm-bands identifying their affiliations, a practice the Court had disapproved, in *dicta*, in *American Communications Association v. Douds* in 1950.[33] The Court then ruled explicitly that forced disclosure of an organization's members and financial supporters restrains free speech and association indirectly by discouraging the exercise of those rights:

It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other] forms of governmental action …. This Court has recognized the vital relationship between freedom to associate and privacy

continued on page 15

continued from page 14

in one's associations …. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[34]

Crediting the NAACP's showing that "on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility,"[35] the Court then rejected the state's argument that citizens are not protected against private reprisals facilitated by government-forced disclosure:

It is not sufficient to answer, as the State does here, that whatever repressive effect compulsory disclosure of names of petitioner's members may have upon participation by Alabama citizens in petitioner's activities follows not from *state* action but from *private* community pressures. The crucial factor is the interplay of governmental and private action, for it is only after the initial exertion of state power … that private action takes hold.[36]

Finally, the Court rejected Alabama's professed need for the membership lists as unconvincing. The Court found that Alabama could establish the NAACP's activities in Alabama through other more obvious sources – including the NAACP's admission that it had engaged in activities in Alabama since 1918.[37]

Significance and Progeny of the Supreme Court's Decision

Clearly, *NAACP* was a watershed decision in the history of the First Amendment. It was definitive in its recognition of the First Amendment right to political privacy. It was a unanimous decision attracting even the support of judicial conservatives. It was a landing pad for the Justices finally to assemble their respective concurring and dissenting opinions over the prior decade. And it trounced state authority because of the obvious recalcitrance of Alabama.

The Court issued the *NAACP* decision on June 30, 1958, a year after its Red Monday decisions in *Sweezy* and *Watkins*, both cited extensively by the NAACP. While the opinion authored by Justice Harlan cited *Sweezy* (including the Frankfurter-Harlan concurring opinion) and *Rumely*, it did not cite *Watkins*, a more modest decision about congressional subpoena pertinence. But *Sweezy* and *Rumely* were advanced in First Amendment jurisprudence.

Because other southern states also were demanding that the NAACP disclose the names of its members and donors, the ruling had a direct application to stopping those efforts in cases like *Bates v. City of Little Rock*,[38] *Louisiana ex rel. Gremillion v. NAACP*,[39] and *Gibson v. Florida Legislative Investigation Committee*,[40] all cases involving forced exposure, in one context or another, of members in civil rights organizations. Each time the Court ruled, it embedded political privacy more deeply into First Amendment jurisprudence.

The decision had less impact on the continuing saga of litigation over communist hunting, as judicial conservatives balked at extending the same analysis to communists, usually by affording greater deference to the government's proffered interest justifying the infringement – national security.[41] Justice Frankfurter was in full retreat after

continued on page 16

continued from page 15

the *Sweezy* decision. In each case where a majority of the Court declined to extend *NAACP* to other contexts, Justice Douglas and Justice Black met them with dissents, often joined by Chief Justice Warren or Justice Brennan. The varying majority and dissenting opinions in that line of decisions are rich in wisdom and inform legal debates in this field today.

The Legacy of *NAACP v. Alabama*

Some modern observers, principally those who support greater exposure of private political associations and funders, argue that *NAACP*'s holding is quite limited to the unique civil rights context. For them, *NAACP* is a decision of quite limited import in today's debates over exposure, transparency, and political privacy.

Yet, stopping there would understate the profound First Amendment importance of *NAACP*. Thousands of court decisions have cited *NAACP* since 1958 in contexts far from the civil rights movement. Surely the same First Amendment protection afforded the NAACP protects the Edward Rumelys and Paul Sweezys as well as all American citizens with equal force.

Moreover, stopping with the civil rights movement would overlook one of the most important extensions of *NAACP* less than two years later, *Talley v. California*,[42] a decision recognizing, for the first time, the First Amendment right to speak anonymously. *Talley* was not a case arising from the civil rights movement in the south. This series will pick up at *Talley* and the right of anonymous speech in the next chapter. ■

For more information on the First Amendment Right of Political Privacy, please contact:

Lee E. Goodman
202.719.7378
lgoodman@wileyrein.com

Endnotes

[1]347 U.S. 631 (1954). Prior to the NAACP's legal problems with Alabama, other civil rights lawsuits funded at least in part by the NAACP had included *Missouri ex rel. Gaines v. Canada*, 305 U.S. 337 (1948); *Smith v. Allwright*, 321 U.S. 649 (1944); *Sipuel v. Board of Regents*, 332 U.S. 631 (1948); *McLaurin v. Oklahoma State Regents*, 339 U.S. 637 (1950); *Sweatt v. Painter*, 339 U.S. 629 (1950); *Mayor v. Dawson*, 350 U.S. 877 (1955).

[2]*Gayle v. Browder*, 142 F. Supp. 707 (M.D. Ala. 1956), *aff'd* 352 U.S. 903 (1956).

[3]For a summary of similar southern state actions to expose members and financial supporters of the NAACP, *see* Jack Greenberg, *Crusaders in the Courts* (Basic Books 1994) at 219-221.

[4]*NAACP v. State of Alabama, ex rel. John Patterson*, 357 U.S. 449, 452 (1958).

[5]*Id.*

[6]*Id.* at 452-453.

[7]*Id.* at 453.

[8]*Id.*

[9]*Id.*

[10]*Id.*

[11]*Id.* at 453-454.

[12]*See* Brief of Petitioner in *NAACP v. Alabama* (1957WL55387 *11).

[13]*Id.*

[14]357 U.S. at 454.

[15]*Id.*

[16]Id.

[17]353 U.S. 972 (1957).

[18]*See* Brief of Petitioner in *NAACP v. Alabama* (1957WL55387 *12).

[19]*Id.* at *15-16.

[20]*Id.* at *17.

[21]*Id.* at *26.

[22]*Sweezy v. New Hampshire*, 354 U.S. 234 (1957).

[23]*Watkins v. United States*, 354 U.S. 178 (1957).

[24]*See* Brief of Petitioner in *NAACP v. Alabama* (1957WL55387).

[25]*United States v. Rumely* 345 U.S. 41 (1953).

continued on page 17

continued from page 16

[26]*See* Reply Brief of Petitioner in in *NAACP v. Alabama* (a pdf copy is available on Westlaw).

[27]*Id*. at 8.

[28]*See* Brief of Respondent in *NAACP v. Alabama* (1957WL55388 *25-27).

[29]*Id*. at *29.

[30]*Id*. at *19-24.

[31]357 U.S. at 459.

[32]*Id*. at 459-460.

[33]*American Communications Association v. Douds*, 339 U.S. 382 (1950). The decision was not a particularly libertarian decision, upholding (by a vote of 5 to 1) the forced administration of anti-communist loyalty oaths for labor union leaders, but it nonetheless included the observation that a "requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously" an infringement of First Amendment rights. The Court seized upon this passage and compared forced disclosure of organizational members to this "obvious" infringement.

[34]357 U.S. at 462.

[35]*Id*.

[36]*Id*. at 463.

[37]*Id*. at 464-465.

[38]*Bates v. City of Little Rock*, 361 U.S. 516 (1960).

[39]*Louisiana ex rel. Gremillion v. NAACP*, 366 U.S. 293 (1961).

[40]*Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539 (1963).

[41]*See, e.g., Beilan v. Board of Public Education*, 357 U.S. 399 (1958) (decided the same day as *NAACP* and upholding school system's dismissal of teacher who refused to answer questions about communist affiliations); *Communist Party of the United States v. Subversive Activities Control Board*, 367 U.S. 1 (1961) (upholding law requiring the Communist Party USA to register with the federal government and disclose membership information because it was directed or controlled by the "world Communist movement").

[42]*Talley v. California*, 362 U.S. 16 (1960).

Events & Speeches

"Just What the Doctor Ordered: Health Law Basics for a Business Law Practice."

ABA Business Law Section Webinar

Kirk J. Nahra, Panelist

February 28, 2019

"The Path Towards a New and Complete Consumer Health Privacy and Security Regulatory Structure."

28th National HIPAA Summit

Kirk J. Nahra, Speaker

March 5, 2019 | Washington, DC

"Regulatory Challenges For Digital Health – The Emerging Law and Filling The Gaps,"

ABA Health Law Section Emerging Issues Conference

Kirk J. Nahra, Panelist

March 13-16, 2019 | Orlando, FL

Privacy Boot Camp

IAPP 2019 Global Privacy Summit

Kirk J. Nahra, Speaker

May 1, 2019 | Washington, DC

"The Privacy and Security Challenges of New Technologies."

PLI Privacy Institute

Kirk J. Nahra, Panelist

May 21, 2019 | New York, NY

Contributing Authors

Lee E. Goodman	202.719.7378	lgoodman@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Duane C. Pozza	202.719.4533	dpozza@wileyrein.com
Joan Stewart	202.719.7438	jstewart@wileyrein.com

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.