Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | February 2019

Our monthly issue continues to explore the growing array of hot topics and broadening reach of privacy and security law. Duane Pozza examines "connected cars" as an enormous new source of personal data. Megan Brown, Duane Pozza, and Boyd Garriott analyze some key recent developments related to privacy and data security class actions. Matthew Gardner, Megan Brown, Michael Diakiwski, and Boyd Garriott consider the implications for supply chain and certain technology issues under new DOJ leadership. And Lee Goodman continues his analysis of the First Amendment right to political privacy. As always, please let us 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. Thank you for reading. ■

ALSO IN THIS ISSUE

Connected Cars and a Deluge of Data

By Duane C. Pozza

Vehicles continue to become more connected – to each other, to surrounding infrastructure, to mobile devices, and to the cloud. New technologies such as 5G will enable faster connectivity and greater functionality. Cars will provide more customized user experiences, enhanced entertainment options, and seamless integration with other Internet of Things (IoT) services. And with this will come much, much more data being collected and shared. Indeed, some observers have projected that fully autonomous vehicles could eventually generate *terabytes* of data a day.

As the amount of data collected and shared increases, privacy and security regulatory concerns will be at the forefront. To date, the

continued on page 2

federal government has largely focused on best practices and industry self-regulation in the areas of privacy and data security in vehicles, rather than regulatory or enforcement actions. But both federal and state regulators have emphasized that privacy and data security enforcement will be priorities, and states in particular have ramped up their enforcement efforts in these areas.[1] And the history of the Federal Trade Commission's (FTC) approach to privacy and security in the area of mobile devices suggests greater scrutiny is coming, as vehicles ramp up and even surpass the amount of data collected and shared by mobile devices.

Federal Efforts to Date

Much of the attention on car connectivity to date has focused on adoption of vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications for the purposes of improving safety.[2] But regulators have acknowledged the potential privacy and security issues surrounding the collection and sharing of certain data, even while avoiding proscriptive solutions. In mid-2017, for example, the National Highway Traffic Safety Administration (NHTSA) and the FTC held a joint workshop on privacy and security issues on connected cars. The FTC subsequently released a staff perspective summarizing the conference and potential issues on its radar.[3]

In general, the U.S. Department of Transportation has largely focused on safety concerns and conceded the policing of privacy issues to the FTC. Its late-2018 guidance on automated vehicles notes, for example, that DOT "takes consumer privacy seriously, diligently considers the privacy implications of our safety regulations and voluntary guidance, and works closely with the [FTC] ... to support the protection of consumer information and provide resources related to consumer privacy."[4]

Potential Privacy and Cybersecurity Issues

Connected vehicles can collect and share a wide range of data – and the potential legal issues can differ depending on the type of data. Notably, the industry has taken steps to adopt best practices in the privacy area. In 2014, the Alliance of Automobile Manufacturers and Association of Global Automakers jointly released Consumer Privacy Protection Principles for vehicle technologies and services.[5] These provide an important anchor as the legal and regulatory landscape around privacy protections continues to evolve. Some key areas of interest include:

Biometric data. Vehicles now have the technology to more closely monitor driver characteristics – for example, sensors that could detect distracted driving. Indeed, the Department of Transportation has suggested that companies are "encouraged to consider whether it is reasonable and appropriate to incorporate driver engagement monitoring in cases where drivers could be involved in the driving task so as to assess driver awareness and readiness to perform the full driving task."[6] Vehicles also can use facial recognition to provide the driver with augmented views or navigation systems.

Collection and use of biometric information can raise issues under some state laws – most notably the Illinois Biometric Information Privacy Act (BIPA), which requires notice and consent to use of certain biometric identifiers.[7] As detailed elsewhere in this

continued on page 3

issue, class action plaintiffs have been litigious in bringing claims under BIPA's private right of action, regardless of whether they can show that consumers were actually harmed by alleged violations. Additionally, FTC staff has noted that vehicles might collect fingerprints or iris patterns, which it views as "sensitive data" – which could suggest higher levels of scrutiny under the FTC's Section 5 authority.[8] The use of biometric data is certainly one area where the legal and regulatory outlook can move quickly, and that will need to be monitored.

Location data. Just as with phones, vehicles can collect detailed information about a person's whereabouts and activities. Some of this information can be used for safety purposes; as the FTC notes, manufacturers can collect "precise geolocation information to direct emergency personnel to the scene of a crash."[9] However, the sharing of location information has drawn congressional scrutiny in the context of mobile devices, with Members of Congress pushing for investigations into the sharing of such data with third parties. In this area, the manufacturers' Privacy Principles require affirmative consent for using geolocation information as the basis for marketing or sharing that information with unaffiliated third parties for their own purposes, including marketing.[10] Companies involved in connected vehicles will want to carefully consider developments in this area.

Commercial data. Vehicles' infotainment systems may collect information about consumers' commercial activities or browsing activities, either by syncing with users' mobile devices or by collecting information though user interaction with the vehicle – such as by providing voice assistance or payment opportunities.[11] This information is potentially valuable to advertisers and can help tailor experiences for consumers. For example, a driver will be able to ask the vehicle's voice assistant for suggestions, and the responses could be tailored to the individual's transaction history.

While this kind of data collection is common on mobile devices, FTC staff has noted some skepticism, writing that "consumers may be concerned about secondary, unexpected uses of such data. For example, personal information about vehicle occupants using the vehicle's infotainment system, such as information about their browsing habits or app usage, could be sold to third parties, who may use the information to target products to consumers."[12] At the workshop, at least for information that was collected by syncing a mobile device, FTC staff's view was that there was a consensus on best practices that "consumers should be provided with clear, easily understandable information about if and how their information is being collected, stored, or transmitted and how they can access or delete that information."[13] Regulators' privacy concerns with mobile devices and infotainment systems may continue to converge as the two platforms increasingly become connected.

Driver behavior data. As the FTC notes, vehicles can collect "information about consumer driving habits, such as if a driver regularly speeds or slams on the breaks." CC at 2. Vehicles might collect such information for safety or operational reasons. The manufacturers' Privacy Principles currently require consent for sharing this kind of information with third parties, such as insurers, who use it for their own purposes,[14] and industry participants may run into more scrutiny if the information is shared outside

continued on page 4

of the context of safety and other limited purposes. FTC staff notes, for example, that one potential benefit of this data collection is that "consumers who demonstrate good driving habits can qualify for insurance discounts," but that "[s]ome participants viewed this use as a benefit rewarding safer driving; others were concerned about the potential for insurance companies to use this information, without consumers' knowledge, to raise rates, or to penalize safe drivers who choose not to authorize the collection of information."[15]

Cybersecurity. Advancements in connectivity and vehicle capability will make cars attractive targets for hackers. The security issues are not limited to hackers attempting to take control of the vehicle in some way; instead, hackers might attempt to access sensitive information that could be used for phishing attempts or other kinds of fraud. Connected vehicles can pose unique cybersecurity challenges. For one, the life cycle for vehicle systems is much longer than for other consumer products – cars typically stay on the road much longer than a consumer typically keeps a mobile phone. Connected vehicle systems need to be capable of being updated over time, including to address vulnerabilities that were not known at the time of manufacturing. And software patches and updates need to be pushed out on an ongoing basis, just as with PCs and mobile devices.

Industry participants are moving toward voluntary best practices and collaborative approaches on information-sharing to enhance cybersecurity across the industry. DOT has encouraged companies to incorporate industry practices on cybersecurity at the design state, and to "establish robust cyber incident response plans."[16] The Automotive Information Sharing and Analysis Center (Auto-ISAC) has, for example, released Automotive Cybersecurity Best Practices, covering governance, risk management, security by design, threat detection, incident response, training, and collaboration with appropriate third parties.[17] And both the FTC[18] and the DOT[19] have endorsed voluntary information sharing of cybersecurity threats through industry groups. These kinds of cybersecurity efforts will be critical as vehicles collect and generate increasing amounts of data and become targets.

Conclusion

The deluge of data generated and shared by vehicles will continue to grow, and policymakers and regulators will no doubt be grappling with how to treat different kinds of data and whether to take more proscriptive actions on privacy or data security. Industry participants have taken the lead in best practices but should remain well aware of how quickly technological developments can push privacy and security issues to the forefront. As has happened with mobile devices, the actions that industry participants are taking now to deal with consumer data will be no doubt be subject to scrutiny going forward. ■

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

continued on page 5

Connected Cars and a Deluge of Data

continued from page 4

Endnotes

[1] *See* Peter S. Hyun and Duane C. Pozza, "Expect Aggressive Consumer-Related Investigations from State AGs," *Corporate Counsel* (Jan. 4, 2019), available at **https://www.wileyrein.com/newsroom-articles-Expect-Aggressive-Consumer-Related-Investigations-from-State-AGs.html**.

[2] *See, e.g.*, Scott D. Delacourt, "Top 5 Takeaways from ITS America 2018 on the V2X Path Forward," WileyConnect, June 7, 2018, available at **https://www.wileyconnect.com/home/2018/6/7/top-5-takeaways-from-its-america-2018-on-the-v2x-path-forward**.

[3] FTC Staff, Connected Cars Workshop: Staff Perspective, January 2018, available at **https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf** ("FTC Staff Perspective").

[4] U.S. Department of Transportation, *Preparing for the Future of Transportation: Automated Vehicles 3.0*, at 19 (October 2018), available at **https://www.transportation.gov/av/3** ("AV 3.0").

[5] The Consumer Privacy Protection Principles are available at **https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf**.

[6] U.S. Department of Transportation, *Automated Driving Systems (ADS): A Vision for Safety 2.0*, at 10 (September 2017), available at **https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf** ("AV 2.0").

[7] 740 ILCS 14/1 *et seq*.

[8] FTC Staff Perspective at 2.

[9] *Id*.

[10] Consumer Privacy Protection Principles at 8.

[11] See Duane C. Pozza, "New Issues Raised by Internet of Things Payments," *Law360* (January 4, 2019), available at **https://www.wileyrein.com/newsroom-articles-New-Issues-Raised-By-Internet-Of-Things-Payments.html**.

[12] FTC Staff Perspective at 2.

[13] *Id*. at 3.

[14] Consumer Privacy Protection Principles at 8; *see also* Auto Alliance FAQ, **https://autoalliance.org/connected-cars/automotive-privacy/#automotive-privacy/what-do-consumers-need-to-know-and-do-to-protect-their-vehicle-information-and-car-data-privacy**.

[15] FTC Staff Perspective at 2.

[16] AV 2.0 at 11.

[17] *See* https://www.automotiveisac.com/best-practices/.

[18] FTC Staff Perspective at 3-4.

[19] AV 3.0 at 17-18.

Creative Pleadings, the Growing Role of the Class Action Bludgeon as the Primary Privacy Regulator, and the Cost to American Innovation

By Megan Brown, Duane Pozza, and Boyd Garriott*

There are numerous different options for how to regulate privacy. The United States has generally taken a collaborative self-regulatory approach. The European Union has opted for a much more onerous regulatory regime in the General Data Protection Regulation (GDPR). There are certainly many options in between those two positions. However, recent years have seen the rise of an altogether new and more heavy-handed American privacy regulatory regime not subject to democratic accountability: class action lawsuits.

The U.S. Supreme Court has traditionally been skeptical of allowing lawsuits to proceed on speculative privacy harms. In a 2013 case , *Clapper v. Amnesty International*, the Court considered a challenge to government surveillance of communications. The plaintiffs were attorneys and activists who engaged in sensitive communications with individuals allegedly likely to be surveilled. The Supreme Court **held** that these plaintiffs lacked standing because it was "highly speculative" that any injury from the surveillance was "certainly impending" because a convoluted chain of events was necessary before the government could or would monitor the plaintiffs' communications.

More recently, in a 2016 case, *Spokeo, Inc. v. Robins*, the Supreme Court considered a plaintiff's suit against a website that allegedly posted incorrect information about him online, in violation of a statute. At issue was standing: The only harm alleged was the statutory violation. The Supreme Court **held** that simply alleging "a bare procedural violation" of a statute cannot satisfy standing where the alleged procedural violation would "result in no harm." The Court declined to lay down a bright-line rule but, as an example, noted that posting "an incorrect zip code" would probably not result in "any concrete harm."

In the intervening years, class action plaintiffs' lawyers have engaged in a series of clever pleadings to bypass the "certainly impending" and concreteness standards laid down in *Clapper* and *Spokeo*, respectively.

In 2015, a group of consumers filed a class action lawsuit in federal court against vehicle manufacturer FCA after *Wired* magazine published an **article** describing how two cybersecurity researchers hacked a Jeep Cherokee in a controlled setting. But there was no allegation that any consumer's vehicle had *ever* been hacked outside of a controlled setting. To get around the "highly speculative" problem from *Clapper*, the lawyers couched their harm as an "overpayment theory," arguing that had the consumers known of the security vulnerabilities exposed by *Wired*, they would have paid less for their vehicles or not purchased them at all. For the time being, the overpayment theory was enough for standing. (We have a full article on *FCA v. Flynn* **here**).

The problems with finding standing in *Flynn* are twofold. First, as noted in a **brief** filed by CTIA-The Wireless Association, Cause of Action Institute, and Association for Unmanned Vehicle Systems International (drafted by one of the authors of this article), the "overpayment theory" is a clear end-run

continued on page 7

continued from page 6

around *Clapper*'s prohibition on speculative harms. Second, there are hundreds of thousands of known vulnerabilities in software and products. In theory, plaintiffs could allege that any one of these vulnerabilities had some effect on consumer behavior, essentially requiring perfect cybersecurity and allowing class action plaintiffs to attempt to extract huge verdicts based on 20:20 hindsight.

In another recent case, the United States District Court for the Northern District of Georgia refused to dismiss a class action suit against Equifax for its 2017 data breach (No. 17-CV-3463). While one should rightfully sympathize with anyone whose identity was compromised due to Equifax's data breach, that is *not* what the class action involves. Rather, the lead plaintiff, "Union Asset Management Holding AG, seeks to represent a *putative class of investors that purchased ... securities of Equifax* ... ." The claim is essentially the finance version of the *Flynn* overpayment theory, alleging that: (1) Equifax materially misrepresented the strength of its cybersecurity protections to investors; (2) that misrepresentation inflated Equifax's stock price; and (3) Equifax's data breach revealed that inflation, caused the stock price to fall, and hurt investors.

Taking this theory to its logical endpoint raises the same issues as in *Flynn*. The theory is not limited to situations involving massive data breaches. Rather, under the Equifax theory, plaintiffs could argue that they have a colorable allegation against any company where (1) an agent of the company represents that it has adequate cybersecurity protections; and (2) a cybersecurity deficiency that the company knew or should have known about becomes public. For example, the court highlighted Equifax's CEO's response to a question at a college that was uploaded to YouTube, where he said that preventing data fraud was a "huge priority." Thus, although *In re Equifax* involved a data breach, the opinion opens the door for plaintiffs to obtain class certification, and attempt to extract massive sums from public companies, by bringing claims that would impose a *de facto* perfect cybersecurity requirement without having to meet Article III standing requirements.

In a pair of cases in the United States District Court for the Northern District of California, plaintiffs are trying to push the limits of Article III standing by utilizing a state law to extract liquidated damages from Facebook (Nos. 3:15-cv-03747 and 3:16-cv-00937). The state law – the Illinois Biometric Information Privacy Act (BIPA) – imposes numerous obligations on private entities that collect biometric information, like fingerprints and retina scans. If the entity fails to meet the requirements of the Act, any person "aggrieved" is provided a "right of action ... against an offending party." The plaintiffs in this litigation are arguing that Facebook's "Tag Suggestions" – which uses facial recognition technology to associate individuals' names with faces in photos – collects users' biometric data without meeting BIPA's procedural requirements, thus entitling plaintiffs to liquidated damages.

Thus far, this standing theory has prevailed. In early 2018, the court refused to dismiss the cases on standing grounds, finding that unlike the mere zip code mentioned in *Spokeo*, a right to privacy of biometric identifiers was (1) "particularly crucial in our digital world because technology

continued on page 8

continued from page 7

now permits the wholesale collection and storage" of these identifiers and they "cannot be changed if compromised or misused"; and (2) the legislature's judgments were well-grounded in "a long tradition of claims actionable in privacy law" under both the "common law and the literal understanding of privacy." Accordingly, the court declined to require plaintiffs to show "real-world harms," paving the way for potential liability by companies using innovative technologies that – as plaintiffs admit – have not actually harmed anyone.

Moreover, even if BIPA's procedural "harms" are eventually held to be inadequate for Article III standing purposes by a federal appellate court, that will not halt the tide of litigation stemming from BIPA. This is because in January, the Supreme Court of Illinois **held** that plaintiffs could state a cause of action under BIPA without "[p]roof of actual damages." (We wrote about this problematic holding **here**). And since state courts, unlike federal courts, are not bound by Article III standing requirements, class plaintiffs will no doubt file their BIPA suits in state courts going forward.

Ultimately, the cases above demonstrate that the most dominant privacy "regulators" are increasingly class action lawyers. But these plaintiffs' lawyers are not bound to the electorate, and their incentive is to extract the largest payout possible for their clients and themselves, *not* to craft the most efficient privacy regulation. This ham-fisted approach to privacy and cybersecurity – if left unchecked – will clutter the dockets of courts and force companies to consider expensive settlements even when there is no actual consumer harm. And this problem is not limited to the Facebooks and the FCAs of the world; **43%** of cyberattacks target small businesses. Accordingly, allowing *ex post* privacy suits with massive damages will have a real and substantial impact on technological development in the American economy writ large.

Applying the blunt instrument of "harm-free" class action lawsuits is simply not the way to vindicate privacy interests. Congress, the federal courts, and state legislatures can and should take action to correct this misguided course. ■

For more information, please contact:

Megan Brown
202.719.7579
mbrown@wileyrein.com

Duane Pozza
202.719.4533
dpozza@wileyrein.com

Boyd Garriott
202.719.4487
bgarriott@wileyrein.com

Boyd Garriott, a Law Clerk in Wiley Rein's Telecom, Media, and Technology practice, contributed to this article.

Tech Companies: Expect DOJ to Be Aggressive on Supply Chain and Tech Under AG Barr

By Matt Gardner, Megan Brown, Mike Diakiwski, and Boyd Garriott*

Attorney General Nominee William Barr weighed in on supply chain risks in his confirmation hearing testimony, previewing a possible extension of the hard line the Administration has taken against what it sees as cyber and economic threats from Chinese companies and the government. Barr testified that China – not Russia – is "the primary rival of the United States," and specifically called out Chinese telecommunications companies Huawei and ZTE.

Barr is hardly new to these issues. After many years of senior government service, he was general counsel of Verizon from 2000 to 2008, so he is no stranger to complex legal, security, and geopolitical issues. He can certainly appreciate the practical challenges that shifting government policy poses to the private sector, as many current U.S. Department of Justice (DOJ) officials do. But if tech firms were hoping Barr's telecom experience might make him more sympathetic to the challenges of monitoring and securing a global supply chain, they may be disappointed. With respect to Huawei and ZTE, Barr testified that, "even in my old Verizon days, we understood the danger and would not use that kind of equipment, even though it would be economically attractive." Barr's statement is consistent with recent actions and statements by the Trump Administration. In April 2018, the Administration imposed significant export restrictions on ZTE and pushed forward with plans to limit Huawei's and ZTE's ability to sell products in the American market. In August 2018, the Defense Authorization Act effectively banned the use of Huawei and ZTE technology by government contractors. Several efforts are underway across the government, and in partnership with the private sector, to address diverse supply chain issues. Myriad efforts in the trade and export control area are percolating as well, with a focus on concerns about Chinese aggression and tactics.

The Administration's recent actions build upon the National Cyber Strategy, which confirms a trend that we have observed in recent years: The government is putting more responsibility on the private sector. While the Strategy outlines rising expectations for government and non-government actors overall, supply chain concerns are featured prominently. Among its first objectives is securing federal networks. "[T]he Administration will centralize some authorities within the Federal Government, enable greater cross-agency visibility, improve management of our Federal supply chain, and strengthen the security of United States Government contractor systems." The Strategy outlines that supply chain risk will be integrated into agency procurement and risk management processes, "in accordance with federal requirements that are consistent with industry best practices[.]" Better information sharing related to supply chain threats will be a priority, and a "supply chain risk assessment shared service" will be created. And the government will also provide streamlined authorities to "exclude risky vendors, products, and services, when justified."

Barr did not signal any retreat from these issues. He praised former Attorney General Jeff Sessions' China Initiative, which was launched in November 2018 and promised aggressive action against Chinese efforts

continued on page 10

Tech Companies: Expect DOJ to Be Aggressive on Supply Chain and Tech Under AG Barr

continued from page 9

to steal U.S. technology. In launching the China Initiative, Sessions called out Chinese economic espionage against the United States and vowed to prioritize Chinese trade secret theft cases, increase enforcement of Foreign Agents Registration Act (FARA) and Foreign Corrupt Practices Act (FCPA) cases against Chinese agents, and "[i]dentify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks." Even before the creation of the China Initiative, the DOJ had been concerned with Chinese technology supply chain issues. In particular, the DOJ created a Cyber-Digital Task Force in February 2018 to assess "the many ways that the Department is combatting the global cyber threat." That Task Force subsequently released a report that found that "[t]echnology supply chains are especially vulnerable, because the hardware components and software code that go into technology products often come from foreign sources, including developers in Russia and China."

If confirmed, technology companies and others should expect Attorney General Barr to knowledgably and aggressively review supply chain issues, in close consultation with the heads of the Criminal Division (Brian Benczkowski) and National Security Division (John Demers). ■

For more information, please contact:

Matt Gardner
202.719.4108
mgardner@wileyrein.com

Megan Brown
202.719.7679
mbrown@wileyrein.com

Mike Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

Boyd Garriott
202.7194487
bgarriott@wileyrein.com

Boyd Garriott, a Law Clerk in Wiley Rein's Telecom, Media, and Technology practice, contributed to this article.

The First Amendment Right to Political Privacy – *Chapter 5—Talley, McIntyre, Jehovah's Witnesses, and the Right to Speak Anonymously*

By Lee E. Goodman

So far, this series has traced the jurisprudential seeds and growth of the First Amendment's protection against forced disclosure of members of private associations, beginning with American communists and following the doctrine through a series of diverse organizations. In Chapter 4, we considered the Supreme Court's unanimous, full-throated ruling in *NAACP v. Alabama* that the First Amendment protects associational privacy. In this Chapter 5, we will pick up with the first significant doctrinal extension of *NAACP,* to protect anonymous speech, in *Talley v. California* and follow that doctrine through a series of opinions decided over the next four decades by solid Court majorities.

From Associational Privacy in *NAACP* to the Right to Speak Anonymously

The NAACP's reply brief in the *Alabama* case was remarkable for the breadth with which it argued an issue that did not appear obvious from the facts of the case. The NAACP's opening brief hewed closely to the Supreme Court's rulings in *Rumely*, *Sweezy*, and *Watkins*, all cases about associational privacy and efforts by organizations to resist exposing their financial supporters and fellow partisans. Associational privacy was the relevant issue in the *Alabama* case too. Yet the NAACP briefed a much broader, and seemingly off track, issue in its reply brief: the right to *speak anonymously*.

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.[1] The NAACP's argument echoed the ideas of Judge Edgerton's dissent in *Barsky v. United States*, which had observed that "[p]ersons disposed to express unpopular views privately or to a selected group are often not disposed to risk the consequences to themselves and their families that publication may entail."[2]

The *NAACP* Supreme Court did not bite. Its decision closely tracked the associational privacy principles articulated in *Rumely* and *Sweezy*. The following year, however, before the ink could dry on the *NAACP* decision, the Court was squarely presented the right to speak anonymously in, *Talley v. California.*

Talley v. California (1960)

Manuel Talley was the Action Director for a Los Angeles-based social justice organization called National Consumers Mobilization.[3] The organization printed handbills urging readers to boycott certain merchants because "they carried products of 'manufacturers who will not offer equal employment opportunities to Negroes, Mexicans, and Orientals.'"[4]

The Los Angeles ordinance provided:

> No person shall distribute any hand-bill in any place under any circumstances, which does not have printed on the cover, or the face thereof, the name and address of the following:
>
> (a) The person who printed, wrote, compiled or manufactured the same.

continued on page 12

continued from page 11

> (b). The person who caused the same to be distributed; provided, however, that in the case of a fictitious person or club, in addition to such fictitious name, the true names and addresses of the owners, managers or agents of the person sponsoring said hand-bill shall also appear.[5]

Mr. Talley was distributing handbills on the street when, upon inspection, Los Angeles officials determined the flyers violated the city ordinance requiring all handbills to post "the names and addresses of the persons who prepared, distributed or sponsored them."[6] Mr. Talley was arrested, convicted of violating the ordinance, and fined $10. His conviction was affirmed by the California appellate court.[7]

In a succinct opinion authored by the First Amendment purist Justice Black, the Court observed "[t]here can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[8] The Court went on to acknowledge the long tradition of anonymous speech in England and the United States, observing that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind"[9] and further that "[i]t is plain that anonymity has sometimes been assumed for the most constructive purposes."[10]

Then, invoking *NAACP* and its offspring, *Bates v. City of Little Rock*, the Court concluded:

> [T]here are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified. The reason for those holdings was that identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance. This broad Los Angeles ordinance is subject to the same infirmity. We hold that it … is void on its face.[11]

The *Talley* decision was decided by a vote of 6 to 3, and the majority opinion was met with a dissenting opinion authored by Justice Clark (joined by Justices Frankfurter and Whittaker). Justice Clark wrote in dissent that "I stand second to none in supporting Talley's right of free speech—but not his freedom of anonymity. The Constitution says nothing about freedom of anonymous speech."[12]

Significantly, the Court struck the ordinance facially while making no mention of any kind of threats or actual retaliation against Mr. Talley, the National Consumers Mobilization organization, or any of its members. In fact, the "record is barren of any claim, much less proof, that [Talley] will suffer any injury whatever by identifying the hand-bill with his name," the dissent lamented. "Unlike [*NAACP*], which is relied upon, there is neither allegation nor proof that Talley or any group sponsoring him would suffer 'economic reprisal, loss of employment, threat of physical coercion [or] other manifestations of public hostility.'"[13]

The unconditional right to political privacy was now definitively established in American jurisprudence, not just in the realm of political association, but in the realm of political and arguably commercial speech (a consumer boycott is arguably commercial speech discouraging consumers from engaging in certain commercial transactions).

continued on page 13

continued from page 12

Talley in Repose

The right of anonymous speech and *Talley* were left in repose for over three decades. In the meantime, the Court's jurisprudence of political privacy meandered through compulsory disclosure rules in discrete contexts, such as making contributions directly to candidates. The most significant decision came in 1976, in *Buckley v. Valeo*, where the Supreme Court upheld the constitutionality of compelled disclosure of financial contributors to federal campaigns for public office as well as those who made independent expenditures to expressly advocate the election or defeat of federal candidates for the objective of preventing corruption of federal officeholders and informing voters of the interests to which they might be beholden.[14] The Court acknowledged the deleterious effects on free speech and association under *NAACP* and *Talley*, but found a sufficient governmental interest justifying compelled exposure of contributors and independent spenders. The Court went further by establishing a special exception for small or unpopular political organizations especially vulnerable to harassment, threats, or reprisals due to dissident beliefs in accordance with *NAACP*.[15]

The Court also endorsed compelled exposure – in *dicta* – in two other cases. In 1978, in *First National Bank v. Bellotti*, the Court struck a state law prohibiting corporations from making expenditures to advocate the passage or defeat of popular referenda, but in a footnote invoking *Buckley* observed that "[i]dentification of the source of advertising may be required as a means of disclosure, so that the people will be able to evaluate the arguments to which they are being subjected."[16]

And in 1981, in *Citizens Against Rent Control v. City of Berkeley*, the Court struck as unconstitutional contribution limits to ballot issue committees, because issues cannot be corrupted in the way that candidates can (*per Buckley*), but in *dicta* observed that "[t]he integrity of the political system will be adequately protected if contributors are identified in a public filing revealing the amounts contributed; if it is thought wise, legislation can outlaw anonymous contributions."[17]

In yet a fourth decision, in 1982, the Court returned to privacy in *Brown v. Socialist Workers '74 Campaign Committee*, which applied *Buckley*'s exception from compelled exposure for minor political parties and harkened to *NAACP*.[18]

McIntyre v. Ohio (1995)

Talley's right to political privacy returned front and center in 1995, when the Court reaffirmed the unadulterated right to speak anonymously by a resounding vote of 7 to 2, with a set of opinions rich in history and legal reasoning.

Margaret McIntyre of Westerville, Ohio, was not a politician or director of a think tank or advocacy organization. She was a regular citizen concerned about the cost of education and tax burdens in her local community. The citizens of Westerville were considering a town referendum to raise taxes in order to increase funding for public schools.

On the evening of April 27, 1988, outside the Blendon Middle School in Westerville, Mrs. McIntyre; her son, a student in the Westerville schools; and a friend distributed leaflets opposing passage of the school

continued on page 14

continued from page 13

tax to be voted on the following week.[19] Mrs. McIntyre distributed the leaflets at the school that evening because the Westerville superintendent of schools was holding a meeting inside the school explaining the merits of the tax. Mrs. McIntyre stood outside the school near the doorway to the meeting room and handed leaflets to people as they entered the building while her son and a friend distributed additional leaflets in the school parking lot by placing them under automobile windshield wipers. The leaflets stated:

VOTE NO

ISSUE 19 SCHOOL TAX LEVY

Last election Westerville Schools, asked us to vote yes for new buildings and expansions programs. We gave them what they asked. We knew there was crowded conditions and new growth in the district.

Now we find out there is a 4 million dollar deficit—WHY?

We are told the 3 middle schools must be split because of over-crowding, and yet we are told 3 schools are being closed—WHY?

A magnet school is not a full operating school, but a specials school.

Residents were asked to work on a 20 member commission to help formulate the new boundaries. For 4 weeks they worked long and hard and came up with a very workable plan. Their plan was totally disregarded—WHY?

WASTE of tax payers dollars must be stopped. Our children's education and welfare must come first. WASTE CAN NO LONGER BE TOLERATED.

PLEASE VOTE NO

ISSUE 19

THANK YOU,

CONCERNED PARENTS

AND

TAX PAYERS

Apparently Mrs. McIntyre's message bothered the superintendent, because he responded to it in the presentation while the assistant superintendent confronted Mrs. McIntyre and informed her that her flyers violated Ohio election laws.

The next evening, on April 28, 1988, a similar school meeting was held at the Walnut Springs Middle School. Mrs. McIntyre appeared outside that school and again distributed her leaflets opposing the school tax levy to persons entering the building to attend the meeting. The assistant superintendent again informed her that the leaflets violated Ohio election laws.

The following week the school tax failed to pass. Subsequently, it was defeated in a second election, but in November of 1988, on the third try, it finally passed.

What ensued was a six-year legal saga. On April 6, 1989, five months after the passage of the school tax referendum, and a year after her leafletting, Mrs. McIntyre received a letter from the Ohio Elections Commission informing her that a complaint had been filed against her by the assistant superintendent, a Mr. Hayfield. She was charged with violating Ohio Revised Code § 3599.09 (as well as two other statutes) because the leaflets she had distributed at the Blendon and Walnut Springs Middle Schools, during the two evenings in April of the previous year, did not

continued on page 15

continued from page 14

contain her name and address. That statute provided (in pertinent part):

> No person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to promote the nomination or election or defeat of a candidate, or to promote the adoption or defeat of any issue, or to influence the voters in any election, or make an expenditure for the purpose of financing political communications through newspapers, magazines, outdoor advertising facilities, direct mailings, or other similar types of general public political advertising, or through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement *the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefore*.[20]

Initially, the charges were dismissed for want of prosecution. A short time later, they were reinstated at the request of the very determined assistant superintendent. On March 19, 1990, a hearing was held before the Ohio Elections Commission, which found Mrs. McIntyre had violated the law by omitting her name from the leaflets. She was fined $100.

Mrs. McIntyre appealed the violation to the Franklin County Court of Common Pleas, which reversed, holding that § 3599.09 was unconstitutional as applied. Subsequently, the Ohio Court of Appeals reversed the Court of Common Pleas and reinstated the fine.[21] That decision was affirmed by the Ohio Supreme Court on September 22, 1993, which concluded the statute and its application to Mrs. McIntyre were well within the bounds of the First Amendment.[22] Both decisions featured majorities and dissents that grappled with the competing lines of Supreme Court authority. The majorities relied more heavily upon *Buckley* while the dissents nodded to *Talley*.

By the time the Supreme Court granted certiorari in the case, Mrs. McIntyre had passed away. Her husband, as executor of her estate, continued the litigation, an indication of the importance of the principles at stake for his late wife and no doubt his interest in her posthumous vindication.

Justice Stevens wrote the opinion of the Court joined by Justices O'Connor, Kennedy, Souter, Ginsburg, and Breyer. Justice Thomas, concurring in the judgment, thought it was important to articulate the First Amendment right under the doctrine of original intent, rather than reasoning the right into existence, and so wrote his own opinion which is a fascinating lesson in early American publishing practices.

The Court held the Ohio law unconstitutional under the First Amendment, because it banned anonymous speech on issues. The Court's analysis drew upon several lines of precedent in reaching this result.

First and foremost, the Court relied on *Talley* for the fundamental principle that the First Amendment protects anonymous speech.[23] Of course, Mrs. McIntyre cited *Talley* throughout her briefs; it was the only

continued on page 16

continued from page 15

precedent cited "passim" in her table of contents.[24]

But the Court found mere citation to *Talley* an inadequate legal analysis and went on to expound on the right to the point of expanding it beyond the boundaries of dissident speech that might be curtailed due to the kinds of threats presented in *NAACP*. In the broadest, most unqualified exposition of the right to speak anonymously, the Court observed:

> Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[25]

Having so broadly conceived of the right, the Court went on to extend it "beyond the literary realm" or even Manuel Talley's call for an economic boycott to the "respected tradition of anonymity in the advocacy of political causes," which the Court analogized to the hallowed right to cast a secret ballot.[26]

Expanding the analysis even further, the Court reasoned that government-compelled disclaimers identifying speakers are a form of forced speech the Court had ruled unconstitutional in *Miami Herald Publishing Co. v. Tornillo*.[27] "[T]he identity of the speaker is no different from other components of the document's content that the author is free to include or exclude," the Court ruled.[28] And from that reasoning the Court conceived of the Ohio law requiring disclaimers of the speaker's identity as a categorical speech ban based on its content. That is, the Court likened anonymous speech as a "category of speech" like any other category and therefore the Ohio statute banned the entire category of speech – speech that chose to exclude from its content the name of the speaker.[29]

Having recognized the First Amendment right (which Justice Thomas asserted was originally intended by the Founders), the Court then considered Ohio's asserted interests in infringing the right under "exacting scrutiny," which required Ohio to prove its ban against anonymous speech was "narrowly tailored to serve an overriding state interest."[30]

Ohio asserted two governmental interests. First, the ban prevented fraudulent and libelous information. Second, the ban provided Ohio citizens relevant information. In support, Ohio naturally relied upon the intervening decision of *Buckley* and the dicta in *Bellotti*.

The Court distinguished the two decisions. First, the Court observed that *Bellotti*'s brief reference to the "prophylactic effect" of exposure was only *dicta* and the Court implied that it might reach only corporate speech,[31] but ultimately disposed of *Bellotti* on the basis that the brief *dicta*

continued on page 17

continued from page 16

relied on *Buckley*. As to that decision, the Court distinguished the government's interest in exposing financial contributors and independent spenders on behalf of candidates for public office, which was at issue in *Buckley*, from speech about issues, at issue in *McIntyre*. People can be corrupted, the Court reasoned, but issues cannot.[32] Mrs. McIntyre's speech was about political issues, and Ohio could not justify infringing her right to express her opinions anonymously.

Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton (2002)

Justice Stevens would be presented another opportunity to cement his concept of First Amendment anonymity in the law seven years later, in yet another pamphleteering case from Ohio. This time, the case was not about political advocacy, but religious proselytizing by Jehovah's Witnesses who desired to distribute religious materials door to door. The Court decided this case by a 8 to 1 vote margin (with only Chief Justice Rehnquist dissenting). The same Justices made up the majority opinion, while this time Justice Scalia joined Justice Thomas in a concurring judgment.

The Village of Stratton, Ohio, had enacted an ordinance that prohibited "canvassers" from "going in and upon" private residential property for the purpose of promoting any "cause" without first having obtained a permit from the village mayor. In order to obtain a permit, the canvasser had to complete a registration form that, among other information, required disclosure of the canvasser's "name and home address" as well as the "name and address of the employer or affiliated organization" sponsoring the canvasser.[33]

The Watchtower Bible and Tract Society of New York published religious literature for the Jehovah's Witnesses ministry. It challenged the ordinance in federal court in Ohio as a violation of the First Amendment for, among other grounds, infringing the right of the Jehovah Witnesses ministry to distribute religious pamphlets anonymously under *McIntyre*. The federal District Court upheld the ordinance with narrowing constructions. The U.S. Court of Appeals for the Sixth Circuit affirmed.[34]

The Supreme Court focused directly upon the ordinance's requirement for the pamphleteer to disclose her name as a condition of obtaining a permit from the mayor and concluded that provision was sufficient to render the ordinance unconstitutional under the First Amendment.[35]

Like *Talley* and *McIntyre*, there was no record of any kind of financial reprisals, threats, or violence. The constitutional right started the analysis and the government failed to carry its burden to justify the infringement.

The Corollary Right to *Listen* Anonymously

Although not mentioned explicitly in *Talley*, *McIntyre*, or *Watchtower*, the decisions observe that the First Amendment protects the speech reaching the marketplace of ideas for the benefit of the listener as much as the speaker. Implicit is the corollary First Amendment right of each citizen to access information.[36] And the right to speak anonymously directly implies a right to *listen anonymously*.

This was essentially the subject of *Rumely* where the Court ruled people have a right to purchase books privately, free from exposure

continued on page 18

continued from page 17

pursuant to congressional subpoena.[37] A decade later, the Court struck a law requiring citizens who wanted to receive "communist political propaganda" to register their names with the U.S. Postal Service.[38] Many lower courts have had occasion to rebuff governmental efforts to pry into citizens' book purchases, library choices, and Internet searches.[39]

Concluding Observations

First Amendment jurisprudence profoundly transformed from 1948, when the D.C. Circuit Court of Appeals denied the existence of a First Amendment right to political privacy and the Supreme Court declined to even hear the issue. Judge Edgerton and Justices Black and Douglas articulated a legal right in the wilderness. But 10 years later, their dissenting concept of the First Amendment right to speak and associate privately, secretly, and anonymously was firmly embedded in Supreme Court interpretation of the First Amendment, and Justice Thomas would opine the right existed from the time of the Founding.

Once recognized, the right would protect conservative anti-New Dealer Edward Rumely, Marxist economist Paul Sweezy, civil rights advocate NAACP, economic justice pamphleteer Manuel Talley, Ohio resident Margaret McIntyre, and the Jehovah's Witnesses. The First Amendment protected a wide range of opinions and organizations, not only dissidents or minority viewpoints. The diversity of these citizens and their causes speaks volumes about how profoundly important this right has been to all Americans to associate privately, speak anonymously, and listen secretly to ideas of their choice.

As definitive as the right to political privacy became, however, a parallel line of First Amendment jurisprudence was evolving which authorized government infringements of the right. *Buckley* and its progeny recognized overriding governmental interests in certain contexts, particularly financial contributions and expenditures to elect candidates. Consequently, as important as the right to political privacy has become, many complicated debates over the metes and bounds of the constitutional protection it actually affords, and the strength of governmental interests that might justify its infringement, persist today. The legal, policy, and political debates are intensifying. Chapter 6 of this series will look at some of the more complicated and controversial contexts, including the difficult issue of campaign finance disclosure. ■

For more information, please contact:

Lee E. Goodman
202.719.7378
lgoodman@wileyrein.com

continued on page 19

continued from page 18

Endnotes

[1] Reply Brief of Petitioner in *NAACP v. Alabama at 8* (a PDF copy is available on Westlaw).

[2] *Barsky v. United States*, 167 U.S. 241, 255 (1948) (Edgerton, *dissenting*).

[3] *See, generally,* Clayborne Carson, *et al.*, eds., *The Papers of Martin Luther King, Jr. Volume III: Birth of a New Age December 1955 – December 1956* (University of California Press 1997) (publishing letter from Dr. King to Mr. Talley discussing bus boycotts) (available online at https://kinginstitute.stanford.edu/king-papers/documents/manuel-d-talley).

[4] *Talley v. California*, 362 U.S. 60, 61 (1960).

[5] Municipal Code of the City of Los Angeles § 28.06 (1958).

[6] 362 U.S. at 63.

[7] *California v. Talley*, 172 Cal.App.2d Supp. 797, 332 P.2d 447 (App. Dept. Los Angeles Co.) (1958).

[8] 362 U.S. at 64.

[9] *Id.*

[10] *Id.* at 65.

[11] *Id.* (citing *NAACP v. State of Alabama*, 357 U.S. 449, 462 (1958) and *Bates v. City of Little Rock*, 361 U.S. 516 (1960)).

[12] *Id.* at 70 (Clark, *dissenting*).

[13] *Id.* at 69 (Clark, *dissenting*) (citing *NAACP v. State of Alabama*, 357 U.S. 449, 462 (1958)).

[14] *Buckley v. Valeo*, 424 U.S. 1, 67-68 (1976).

[15] *Id.* at 73-74.

[16] *First National Bank v. Bellotti*, 435 U.S. 765, 792 n. 32 (1978).

[17] *Citizens Against Rent Control v. City of Berkeley*, 454 U.S. 299-300 (1981). The issue before the Court was the constitutionality of Section 602 of City of Berkeley Election Reform Act of 1974, Ord. No. 4700-N.S. In striking that provision, the Court observed that another ordinance, Section 112, which required public disclosure of all donors to a ballot measure committee, adequately served the City's purported interests. But this was *dicta* because the constitutionality of Section 112 was not before the Court.

[18] *Brown v. Socialist Workers '74 Campaign Committee*, 459 U.S. 87, 91-93 (1982).

[19] The facts are restated from the Petitioner's Brief in *McIntyre v. Ohio*.

continued on page 20

continued from page 19

[20] Ohio Revised Code § 3599.09 (1988) (emphasis added).

[21] *McIntyre v. Ohio Elections Commission*, 1992 WL 230505 (Ohio App. 10th Dist., April 7, 1992).

[22] *McIntyre v. Ohio Elections Commission*, 67 Ohio 391, 618 N.E.2d 152 (1993).

[23] 514 U.S. at 341-342 (*quoting Talley*).

[24] Petitioner's Brief in *McIntyre v. Ohio* (1994 WL 144557).

[25] 514 U.S. 341-342 (emphasis added).

[26] *Id.* at 342-343.

[27] *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241 (1974).

[28] *Id.* at 348.

[29] *Id.* at 357.

[30] *Id.* at 347.

[31] *Id.* at 353-354. To the extent the Court, in 1995, implied that corporations might not have First Amendment protections or might be subject to discriminatory infringements of speech rights, that analysis would not withstand the force of the Court's 2010 decision in *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010).

[32] *Id.* at 354-356.

[33] Village of Stratton Ordinance No. 1998-5, Sections 116.01, 116.02, 116.03 (1998).

[34] 240 F.3d 553 (2001).

[35] *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166-167 (2002).

[36] *See, e.g., Packingham v. North Carolina*, 137 S.Ct. 1730, 173 (2017) ("A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more.... [T]he statute here enacts a prohibition unprecedented in the scope of First Amendment speech it burdens. Social media allows users to gain access to information and communicate with one another about it on any subject that might come to mind.... In sum, to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights. It is unsettling to suggest that only a limited set of websites can be used even by persons who have completed their sentences. Even convicted criminals—and in some instances especially convicted criminals—might receive legitimate benefits from these means for access to the world of ideas."); *United States v. Playboy Entertainment Group,*

continued on page 21

continued from page 20

Inc., 529 U.S. 803, 817 (2000) ("The citizen is entitled to seek out or reject certain ideas or influences without Government interference or control."); *Bd. of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (stating that the right to receive information is "an inherent corollary of the rights of free speech and press" because "the right to receive ideas follows ineluctably from the sender's First Amendment right to send them" and because the right is "a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press, and political freedom."); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Griswold v. Connecticut*, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read ... and freedom of inquiry...."); *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943) ("The right of freedom of speech and press has broad scope.... This freedom embraces the right to distribute literature ... and necessarily protects the right to receive it.").

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

[38] *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965).

[39] *See, e.g.*, *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (2002) (collecting authority); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. L. Rev. 981 (1996) (collecting authority).

Contributing Authors

Megan L. Brown	202.719. 7579	mbrown@wileyrein.com
Michael L. Diakiwski	202.719. 4081	mdakiwski@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Boyd Garriott	202.719.4487	bgarriott@wileyrein.com
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

Boyd Garriott, a Law Clerk in Wiley Rein's Telecom, Media, and Technology practice, contributed to this newsletter.