JUDGE WYNN AND TECHNOLOGY*

RICHARD PELL**

Judge Wynn stands out in the judiciary for his eagerness to gain a deep understanding of novel technological issues. In thirty years on the bench, he has maintained a focus on the effects of emerging technology on the law, particularly as technological advances impact civil liberties and reshape the balance of power between the individual and the state along demographic and socioeconomic lines.

I. THE NEED FOR INFORMED LEGAL DECISIONS ON TECHNOLOGICAL ISSUES

Technological issues often run afield of traditional judicial education and training and, for that reason, are sometimes constrained or channeled to discrete jurisdictional enclaves. For instance, the Court of Appeals for the Federal Circuit hears all patent appeals. But most judges are general practitioners who face a wide variety of cases—from contract interpretation to criminal sentencing to constitutional disputes. The details of those lawsuits vary along many dimensions. They may involve everyday facts, such as what happened during a physical search of a house by police. They may also turn, in critical ways, on an understanding of novel technologies, such as the methods by which facial recognition software matches a suspect to an image in a photo lineup. Because we live in a time of exponential[1] and recombinant growth[2] in digital technologies—meaning that a large array of easily replicated technologies can be mixed and matched to produce new ideas and products—technical advances often outpace the knowledge or understanding of professionals employed full-time in technical fields. The situation is even more challenging for the judiciary, which skews older and may lack exposure to, or familiarity with, new technologies. It follows that judges may not readily grasp new concepts and structures that emerge from the growth of networked digital technologies, from

** Richard Pell clerked for Judge Wynn from 2019 to 2020. He thanks his fellow clerks—McKenna Jacquet-Freese, Aislinn Klos, and Anna Peterson—for their assistance in preparing and editing this piece. He also thanks Allison Nicole Schmidt and the staff of the *North Carolina Law Review* for their excellent editorial review. The views expressed herein are the author's own and do not reflect the views of Judge Wynn or any employer.

1. *See* David R.S. Cumming, Stephen B. Furber & Douglas J. Paul, *Beyond Moore's Law*, 372 PHIL. TRANSACTIONS ROYAL SOC'Y, Mar. 2014, at 1, 1–2 (explaining reasons for exponential growth in digital computing power and associated technologies).

2. *See* Martin L. Weitzman, *Recombinant Growth*, 113 Q.J. ECON. 331, 333 (1998).

TikTok videos, Twitter, internet memes, and e-commerce, to complex government surveillance techniques and crime-prediction tools.

Yet, the judiciary cannot avoid issues of a technical nature, as digital technologies continue their relentless march into every corner of contemporary life, creating novel cases and controversies. And the stakes are high. A cursory glance at the news reveals an ongoing "parade of horribles"[3] arising from the proliferation of digital data and technologies built on it. Unvetted machine learning systems used in so-called "predictive policing" initiatives aim to anticipate crime, but instead, merely justify aggressive law enforcement presence in neighborhoods identified as "high crime."[4] Opaque algorithmic techniques—developed by private enterprise with little oversight—mine social media and public records to assign individuals "threat scores" used by police responding to calls.[5] Police departments rely on biased facial recognition algorithms, despite their high false-positive rates for people of color.[6] Researchers tout the perceived objectivity of computer algorithms which (they claim) can predict individuals' potential for criminality by scanning their faces—a modern spin on the skull-bump phrenology of yore.[7] Surveillance devices designed for anti-terror efforts overseas are deployed in secret by local law enforcement to track all individuals in broad areas and to jam and intercept

3. Oral Argument at 57:17–57:19, Andrews v. Balt. City Police Dep't, 8 F.4th 234 (4th Cir. 2020) (No. 18-1953), https://www.ca4.uscourts.gov/OAarchive/mp3/18-1953-20200128.mp3 [https://perma.cc/LS57-3XGZ] (noting potential "horribles" arising from technological progress).

4. *See* Elizabeth E. Joh, *Feeding the Machine: Policing, Crime Data, & Algorithms*, 26 WM. & MARY BILL RTS. J. 287, 300–01 (2017); WALTER L. PERRY, BRIAN MCINNIS, CARTER C. PRICE, SUSAN C. SMITH & JOHN S. HOLLYWOOD, RAND CORP., PREDICTIVE POLICING: THE ROLE OF CRIME FORECASTING IN LAW ENFORCEMENT OPERATIONS 118–25 (2013), https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf [https://perma.cc/P855-EXDP]; *see also* Mark Joseph Stern, *Black Judge Has To Explain to White Colleague Why Racial Profiling Is Bad*, SLATE (July 16, 2020), https://slate.com/news-and-politics/2020/07/gregory-wilkinson-racial-profiling-fourth-amendment.html [https://perma.cc/N9NQ-ZAJJ].

5. *See* Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score,'* WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html [https://perma.cc/SR5W-M5RG (dark archive)].

6. *See* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU N. CAL. (July 26, 2018), https://www.aclunc.org/blog/amazon-s-face-recognition-falsely-matched-28-members-congress-mugshots [https://perma.cc/E72X-NSMR]; Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/9BX8-X6UR (dark archive)].

7. *See HU Facial Recognition Software Predicts Criminality*, HARRISBURG U. SCI. & TECH. (May 5, 2020), http://archive.is/N1HVe [https://perma.cc/R3SF-CKK4] (claiming to predict a person's propensity for criminal activity from their facial features, similar to the early nineteenth century pseudoscience of phrenology, which claimed to predict human personality traits and intelligence based on the shapes of individuals' skulls). *But see Abolish the #TechToPrisonPipeline*, COAL. FOR CRITICAL TECH. (June 23, 2020), https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16 [https://perma.cc/A5C6-TESC (staff-uploaded archive)].

cell phone communications at peaceful protests.[8] Law enforcement uses smartphone and GPS trackers to achieve a "near perfect surveillance" that monitors individuals' locations with previously unimaginable precision.[9] Government programs have accumulated massive datasets about individuals' everyday activity via Section 215 of the USA PATRIOT Act,[10] Section 702 of the Foreign Intelligence Surveillance Act ("FISA"),[11] and numerous national security policy directives and presidential executive orders.[12] Government entities have likewise compelled disclosure of data from private enterprise under FISA Section 702[13] or purchased such information outright from data brokers—information that would typically require a warrant for the government to obtain it directly.[14]

8. *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 11–12 (2014); Kim Zetter, *How Cops Can Secretly Track Your Phone*, INTERCEPT (July 31, 2020, 7:00 AM), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [https://perma.cc/C4DY-UETN (dark archive)].

9. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

10. *See* Mattathias Schwartz, *Three Big Questions About the NSA's Patriot Act Powers*, NEW YORKER (June 2, 2015), http://www.newyorker.com/news/news-desk/three-big-questions-about-the-n-s-a-s-patriot-act-powers [https://perma.cc/7PMB-D3RR (dark archive)] (describing widespread collection of Americans' telephone metadata under the Patriot Act, including the now-expired Section 215).

11. *See* Sarah St. Vincent, *Warrantless Surveillance Under Section 702 of the FISA Amendments Act: Myths and Facts*, CTR. DEMOCRACY & TECH. (Oct. 9, 2015), https://cdt.org/insight/warrantless-surveillance-under-section-702-of-the-fisa-amendments-act-myths-and-facts [https://perma.cc/X7X7-4A85] (describing how FISA permits law enforcement to siphon off internet-based communications as they pass through network infrastructure).

12. *See* Declan McCullagh, *U.S. Gives Big, Secret Push to Internet Surveillance*, CNET (Apr. 24, 2013, 8:59 AM), http://www.cnet.com/news/u-s-gives-big-secret-push-to-internet-surveillance [https://perma.cc/RP95-JTKK]; John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, WASH. POST (July 18, 2014), https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html [https://perma.cc/2G2N-DKGG (dark archive)].

13. *See* St. Vincent, *supra* note 11.

14. *See* Kate Cox, *Secret Service Buys Location Data That Would Otherwise Need a Warrant*, ARS TECHNICA (Aug. 17, 2020, 3:39 PM), https://arstechnica.com/tech-policy/2020/08/secret-service-other-agencies-buy-access-to-mobile-phone-location-data/ [https://perma.cc/KZ2C-AR4J]; Ashkan Soltani, Andrea Peterson & Barton Gellman, *NSA Uses Google Cookies To Pinpoint Targets for Hacking*, WASH. POST (Dec. 10, 2013), https://web.archive.org/web/20220103181930/https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/ [https://perma.cc/7DAF-V7GH (dark archive)]; U.S. SENATE COMM. ON COM., SCI., & TRANSP., OFF. OF OVERSIGHT & INVESTIGATIONS, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 29 (2013), http://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf [https://perma.cc/7XYW-S2M8].

These problems are not limited to government action. Social media is used to foster hate speech[15] and as a vehicle for election interference and revolt.[16] Corporations of all stripes gather and catalog, down to the most intimate detail, every action each individual takes online in order to build user-specific advertising profiles.[17] Myriad technologies track individuals across each internet-connected device they own.[18] For instance, it is now common for mobile applications and websites to track users' every screen tap and mouse movement, as well as every letter they type.[19] The information gathered is used to classify individuals along sensitive lines, such as race, sexual orientation, socioeconomic status, and health conditions.[20]

Accordingly, when it comes to a world awash in data[21] and new technologies that leverage such data to reshape society and civil liberties, courts must: identify the legal and ethical issues at stake; understand the technology at issue in order to make sound legal rulings; and appreciate the implications of legal rulings on future technological advances and individual rights.

15. *See* Barrie Sander, *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, 43 FORDHAM INT'L L.J. 939, 982–83 (2020).

16. *See* Siladitya Ray, *This Is How Social Media Platforms Plan To Tackle Election Day and Its Fallout*, FORBES (Nov. 2, 2020, 1:05 PM), https://www.forbes.com/sites/siladityaray/2020/11/02/this-is-how-social-media-platforms-plan-to-tackle-election-day-and-its-fallout/?sh=53d6ddba599f [https://perma.cc/9U3W-PAE5 (staff-uploaded, dark archive)]; Davey Alba, *How Russia's Troll Farm Is Changing Tactics Before the Fall Election*, N.Y. TIMES (Mar. 29, 2020), https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html [https://perma.cc/2W25-C3HK (dark archive)].

17. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/PUU5-JJNR (dark archive)].

18. *See How To Protect Your Privacy Online*, FED. TRADE COMM'N CONSUMER ADVICE (May 2021), https://consumer.ftc.gov/articles/how-protect-your-privacy-online [https://perma.cc/96C2-6DFE].

19. *See Online Tracking and Behavioral Profiling*, ELEC. PRIV. INFO. CTR. (2020), https://web.archive.org/web/20211013042910/https://epic.org/privacy/consumer/online-tracking/ [http://perma.cc/CB7K-LFMU]; *see also* Phil Gross, *Cookies, Tags, and Pixels: Tracking Customer Engagement*, VISUAL IQ (Sept. 2012), https://web.archive.org/web/20130918031848/http://www.visualiq.com/resources/marketing-attribution-newsletter-article/cookies-tags-and-pixels-tracking-customer-engagement [http://perma.cc/9LM4-3QGJ]; Dan Goodin, *Beware of Ads That Use Inaudible Sound To Link Your Phone, TV, Tablet, and PC*, ARS TECHNICA (Nov. 13, 2015, 1:00 PM), http://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc [http://perma.cc/68ZV-WGU5].

20. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at iv–v (May 2014), https://www.ftc.gov/system/files/documents/reports/data-broker-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/WK94-EHTS].

21. *See* Åse Dragland, *Big Data, for Better or Worse: 90% of World's Data Generated over Last Two Years*, SCI. DAILY (May 22, 2013), http://www.sciencedaily.com/releases/2013/05/130522085217.htm [https://perma.cc/WY88-VA3P]; Bernard Marr, *Google's Nest: Big Data and the Internet of Things in the Connected Home*, FORBES (Aug. 5, 2015, 10:52 AM), http://www.forbes.com/sites/bernardmarr/2015/08/05/googles-nest-big-data-and-the-internet-of-things-in-the-connected-home [https://perma.cc/T6W2-VTA6 (dark archive)].

II. THE DIFFICULT MARRIAGE OF TECHNOLOGY AND THE LAW

At first blush, Judge Wynn might seem an unlikely candidate to conduct a deep dive in this area because he did not grow up with the privileges of modern technology. He often regaled his clerks with tales of his youth on his family farm in Robersonville, North Carolina—of collecting wood for the stove that heated his house or of drawing buckets of water from the well and carrying them to the house on laundry days. Individuals who grew up on rural farms in the 1950s, like Judge Wynn, typically face structural disadvantages when it comes to grasping new technology.[22]

But Judge Wynn is undeterred. Part of his willingness to dive into technological issues comes from his innate curiosity. Clerks' lunchtime chats with him often involved discussions of how cell phones and computers work, new gadgets, or popular science and engineering topics he had heard about on podcasts. He likewise wanted to know how his clerks—who averaged less than half his age—interacted with "new media"—that is, how we used social media or got our news. Judge Wynn is rarely seen in chambers without his iPad, which he uses for almost every task. He uses a tablet on the bench to communicate with his clerks via instant message during oral arguments—one of only a few judges on the Fourth Circuit to do so. He also serves on the circuit's IT committee, where he is responsible for overseeing digital privacy and security issues.

Judge Wynn's willingness to engage with technology primarily arises from his pragmatic, facts-first approach to every case. He believes that the facts must always dictate what the law should be, and that the more one understands the facts of a case, the less necessary it becomes to rely on sweeping legal principles to justify a decision. In that respect, Judge Wynn is in line with Judge Posner and other pragmatic legal scholars—he aligns with those who judge based on "a rejection of the idea that law is something grounded in permanent principles and realized in logical manipulations of those principles, and a determination to use law as an instrument for social ends."[23]

Finally, Judge Wynn goes on red alert at any whiff of encroachment upon civil liberties or individual dignity. Digital technologies that better arm the state to infringe upon constitutional rights or transfer control of data and personhood from the individual to corporate or state interests are always on his radar.

Judge Wynn's facts-based approach is particularly suited to technological controversies because such cases often present questions of first impression, in that the issues presented involve concepts, structures, and abstractions that have not appeared in the caselaw. In that circumstance, it is often necessary to reason

22. *See* Miriam A. Cherry, *Age Discrimination in the On-Demand Economy and Crowdwork*, 40 BERKELEY J. EMP. & LAB. L. 29, 51 (2019).

23. *See* RICHARD A. POSNER, OVERCOMING LAW 405 (1995).

primarily from the facts because precedent or entire bodies of legal doctrine developed for a separate pattern of facts may not bear on the issue at bar.

But in such unfamiliar terrain, judges—and the lawyers who brief them—often do the natural thing: they reach for what they know. In the context of technology, this frequently means resorting to analogies to familiar, nontechnological ideas to conceptualize a new or intimidating topic.[24] This practice results in a variety of absurd analogies in technical settings—from legislators describing the internet as a "series of tubes"[25] to U.S. Supreme Court Justices likening GPS trackers on cars to "tiny constable[s]" riding on stagecoaches in 1791.[26]

Judge Wynn's pragmatism leads him to conclude that the legal issues can only be decided after the court understands the technology on its own terms. As such, he is wary of analogies for several reasons. First, they are unlikely to encompass all behaviors of a technological system and instead omit crucial details in an effort to simplify. Second, analogies usually take on lives of their own and cease to reflect the technology they purport to describe.[27] Third, analogies cannot define technological structures or concepts that lack a ready counterpart in common—or legal—experience. As a result, Judge Wynn believes judges and counsel must engage with technical concepts directly, without the comforting proxy of analogy, in order to gain "native" fluency in the concepts and vocabulary of the relevant technical domain.

That is not to say that Judge Wynn refuses to use analogy as a rhetorical device to communicate technical topics. He simply believes that any such analogy must flow from a "look under the hood" at the technical facts of a particular case because a judge cannot ascertain whether an analogy offered by a party is apt until he or she understands the technology at issue and the extent to which the proffered comparison reflects technical reality.

24. *See* Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741, 745 (1993).

25. Andrew Seitz, *It's a Series of Tubes: Network Neutrality in the United States and How the Current Economic Environment Presents a Unique Opportunity To Invest in the Future of the Internet*, 29 J. NAT'L ASS'N ADMIN. L. JUDICIARY 683, 708–09 n.172 (2009) (contextualizing Senator Stevens' infamous statement of the internet as a "series of tubes").

26. United States v. Jones, 565 U.S. 400, 420 n.3 (2012) (Alito, J., concurring).

27. Although not technical in nature, the 2019–2020 clerks saw an analogy stretched to its breaking point in real time at a Fourth Circuit oral argument. The case was *In re Trump*, 958 F.3d 274 (4th Cir. 2020)—a suit alleging the President illegally received emoluments through a hotel he owned in the District of Columbia. *Id.* at 280. In rejecting the case as nonjusticiable because the plaintiffs hesitated to articulate a remedy at the pleadings stage, a judge, in passing, compared their case to getting on an airplane without knowing where it is going. Oral Argument at 1:32:15–1:32:28, *In re Trump*, 958 F.3d 274 (No. 18-2486), https://www.ca4.uscourts.gov/OAarchive/mp3/18-2486-20191212.mp3 [https://perma.cc/2H8A-CVPL]. Unable to resist the bait, plaintiffs' counsel asserted that, at the least, the plaintiffs had "gotten through TSA" and should be "allowed to board their plane." *Id.* at 1:33:05–1:33:10. Opposing counsel, feeling the need to respond, stated that it was "clear that airplane's gonna crash." *Id.* at 1:45:23–1:45:28. Although slightly amusing and diverting, these analogies did not address the case's actual procedural posture.

III. FACTS-FIRST APPROACH TO TECHNOLOGY DISPUTES

This facts-based approach to technology disputes shines through in a variety of Judge Wynn's cases. His dissent in *United States v. Bosyk*[28] is most illustrative.[29] There, the police monitored a message board that was known for featuring child pornography.[30] At an unspecified time on November 2, 2015, a post on that bulletin board identified a particular child pornography video, shared a set of thumbnail images captured from the video, listed a URL, stated that the URL pointed to the video, and provided an accompanying password.[31] The URL, in turn, linked to a file on a third-party file-sharing website, which hosted a downloadable copy of the password-protected video of child pornography.[32] Law enforcement subpoenaed the third-party site for records of who had downloaded the video and discovered that on November 2, 2015, a computer with the defendant's IP address attempted to download the video.[33] That is, the defendant's computer attempted to access the URL, which was in a nondescriptive form: http://[redacted].comxu5me9erdipp/brochure.rar.html.[34]

What the police could not prove was whether the IP address that attempted to access the third-party link reached the link through the post on the bulletin board—which identified the linked file as child pornography—or if it accessed the link some other way, such as by a post elsewhere which may or may not have accurately identified its contents.[35] The panel majority decided that because the defendant's IP address attempted to download the video by accessing the URL on the same day that the URL was posted on the bulletin board, the police had enough information for probable cause and a search warrant.[36] Implicit in that reasoning was the assumption that, because the police had only observed the URL on the bulletin board, any person accessing the URL must also have come across it on the bulletin board and therefore must have seen the description of the linked video as child pornography.

Judge Wynn faulted the majority for not fully engaging with the relevant technology, noting that, as a matter of common sense, URLs are readily replicated across the internet and it is easy to click a nondescript link without knowing that it will lead to objectionable or illegal content. He wrote that

> users can *encounter* URLs . . . through websites, emails, chats, text messages, comment threads, discussion boards, File Sharing Sites (such

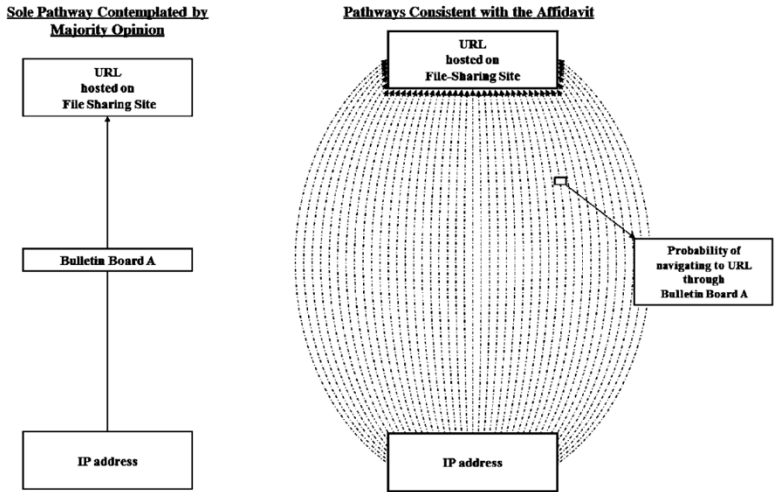
28. 933 F.3d 319 (4th Cir. 2019), *cert. denied*, 140 S. Ct. 1124 (2020).
29. *Id.* at 334 (Wynn, J., dissenting).
30. *Id.*
31. *Id.* at 334–35.
32. *Id.* at 335.
33. *Id.* at 355.
34. *Id.* at 334.
35. *See id.* at 355.
36. *Id.* at 325.

> as DropBox, Google Drive, or Apple iCloud), tweets, Facebook posts, Instagram captions, Snapchat messages, embedded images or videos, unwanted pop-up windows, any combination thereof, or by any other digital means.[37]

Judge Wynn also observed that a URL "can be copied with only a click of a button" and thus could be "further disseminated through any or all of these ways millions of additional times, often in a matter of seconds."[38]

Accordingly, Judge Wynn concluded that "there are myriad ways users can encounter and navigate to a URL—including unintentionally, particularly when, as here, the text of the URL provides no indication as to the nature of the content to which it navigates."[39] In order to simplify the discussion and to illustrate the extent to which the majority ignored alternative pathways by which a user might encounter the URL, Judge Wynn provided an illustration[40]:

Figure 1. Pathways to a URL



Judge Wynn tends to write for a lay audience rather than a legal one. So, once he was comfortable with his understanding of the technical facts, he provided a real-world hypothetical, grounding the technology in an everyday scenario: a grandmother receiving an email from what appeared to be a close friend stating, "Click HERE for my favorite knitting website," where the word "HERE" was a URL pointing to the video.[41] Noting that no reasonable person

37. *Id.* at 343.
38. *Id.*
39. *Id.* at 346.
40. *Id.* at 347.
41. *Id.* at 362.

would understand the content to which the URL referred given its "random alphanumeric string," Judge Wynn stated that if "Grandma" clicked the link, the police would have the same amount of information for a search warrant against Grandma as they used to justify probable cause for a search of the *Bosyk* defendant's home.[42]

Characteristically, Judge Wynn stuck to his guns on the defendant's petition for rehearing en banc, providing the lone vote for granting rehearing, which he accompanied with a written explanation. That statement provides the clearest articulation to date of his approach to technology. He first noted courts' hesitance to approach technical topics: "To many courts, the internet is abstract and the task of learning what a URL is . . . represents a specialized undertaking unrelated to legal expertise, that is, something to approach with a sense of dread."[43] He then addressed the shortcomings of analogical reasoning, noting that analogies "that promise to reduce a technical issue to something susceptible to the intuitive logic of the familiar become appealing," particularly where "retrospective confirmation, such as when we can look back and see that an affidavit led to a computer filled with child pornography, builds trust that the logic [of the analogy] . . . was sound in the first instance."[44] Finally, he concluded that such an approach leads to perverse results in technology cases because "the preference to avoid taking the internet on its own terms, to avoid learning new rules and starting from logical scratch, leads us to not question basic assumptions when we should."[45]

IV. EVOLVING FOURTH AMENDMENT PROTECTIONS IN THE FACE OF NEW TECHNOLOGY

Judge Wynn is alert to technical advances in police surveillance that erode Fourth Amendment privacy protections. Often, that erosion is a result of the third-party doctrine, which exempts any information voluntarily disclosed to a third party from the Fourth Amendment's warrant requirement. This part first provides a brief summary of Fourth Amendment protections in the face of technology and the ways in which historical precedent is ill-suited to networked digital technologies. This part then discusses some of Judge Wynn's forward-looking decisions in this area.

42. *Id.* at 362–63.

43. United States v. Bosyk, 786 F. App'x 398, 399 (4th Cir. 2019) (Wynn, J., dissenting from denial of rehearing en banc).

44. *Id.*

45. *Id.*

A. *Technological Surveillance and the Fourth Amendment*

The jumping-off point for modern Fourth Amendment technological surveillance jurisprudence is a concurring opinion in *Katz v. United States*,[46] in which Justice Harlan articulated a reasonableness standard for what type of surveillance constitutes a Fourth Amendment search.[47] If an individual has a subjective expectation of privacy in some activity and if that expectation is one that society recognizes as objectively reasonable, then surveillance of that activity constitutes a Fourth Amendment search and requires a warrant.[48]

One consequence of *Katz*'s subjective prong is the third-party doctrine: an individual cannot have an expectation of privacy in information she voluntarily conveys to a third party.[49] The U.S. Supreme Court and circuit courts have applied this doctrine to permit warrantless surveillance of telephone numbers dialed,[50] airborne observation,[51] use of electronic tracking devices,[52] collection of email metadata and website address histories,[53] and collection of internet service provider subscriber information.[54] The third-party doctrine is particularly relevant to digital data, the overwhelming majority of which is conveyed to third parties through network routing, cloud storage, and online transactions.

Legal commentators have long criticized the *Katz* test, and that criticism has increased as digital technologies become ubiquitous.[55] The primary critique is that the test assesses societal privacy expectations by reference to current

46. 389 U.S. 347 (1967).

47. *See id.* at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

48. *See id.*; *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979); Kyllo v. United States, 533 U.S. 27, 31 (2001); Soldal v. Cook County, 506 U.S. 56, 68 (1992); Oliver v. United States, 466 U.S. 170, 180 (1984).

49. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.").

50. *Smith*, 442 at 742.

51. *See* Florida v. Riley, 488 U.S. 445, 451–52 (1989); California v. Ciraolo, 476 U.S. 207, 214–15 (1986).

52. *See* United States v. Karo, 468 U.S. 705, 727–28 (1986); United States v. Knotts, 460 U.S. 276, 285 (1983).

53. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (holding that warrantless surveillance of email metadata is not a Fourth Amendment search); *see also* United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (holding that the use of a third-party file-sharing software negated any expectation of privacy of the files accessible by the software). *But see* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (holding that an email's contents were protected by the Fourth Amendment).

54. *See* United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (holding that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (same).

55. *See, e.g.*, Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1386, 1401–03 (2008).

social behavior.[56] This results in circularity: technological progress—including data proliferation that enables novel surveillance techniques—shapes social privacy expectations.

In addition to this hint of technological determinism, the *Katz* test's circularity is also driven by the state of the law—that is, by currently permissible surveillance techniques.[57] This creates perverse incentives for law enforcement to deploy privacy-reducing technologies in secret. Indeed, police departments have gone to great efforts to conceal their use of certain surveillance devices, entering into rigid nondisclosure agreements with suppliers and dismissing criminal cases to avoid disclosing such devices' existence.[58] Similarly, police have an incentive to conduct widespread surveillance in public areas—such as use of closed circuit television ("CCTV") security cameras—to create a "carry-over" reduction in privacy expectations in nonpublic areas: if the government may surveil freely in public, that also shapes perceptions of what the government may properly see in private.[59]

The U.S. Supreme Court has recognized *Katz*'s circularity in the specific context of new surveillance technologies that are not publicly available. In *Kyllo v. United States*,[60] the police used an infrared scanner to determine that the heat signature emanating from the defendant's house was consistent with use of marijuana grow lamps.[61] The Court noted that it "would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[62] Accordingly, the Court used the rarity of the surveillance technology at issue to cabin the privacy reductions resulting from the *Katz* test's circularity, stating that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without 'intrusion into a constitutionally protected area' . . . constitutes a search—at least where (as here) the technology in question is not in general public use."[63] However, this limiting principle does not apply when surveillance-enabling technologies are available to the public—though the Supreme Court has not clarified what it means for a

56. *See id.* at 1386–96.

57. *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

58. *See* United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, C.J., dissenting).

59. *See* Monika Zalnieriute, *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, 22 COLUM. SCI. & TECH. L. REV. 284, 286–87 (2021) (noting that the United States and China have the highest number of surveillance cameras per capita); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1956–57 (2013) (discussing carryover reduction in privacy from CCTV usage in Britain).

60. 533 U.S. 27 (2001).

61. *Id.* at 30.

62. *Id.* at 33–34; *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 827–28 (2004).

63. *Kyllo*, 533 U.S. at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)); *see also* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

technology to be "available." But at the least, money is no object—the Court has held that police use of a helicopter to peer into a defendant's greenhouse did not violate a reasonable expectation of privacy because helicopters, although very expensive, are available for public use.[64]

Another common critique of *Katz* is that its reasonableness standard is not well suited to a period of rapid technological growth.[65] Although judicial determinations of reasonableness are certainly routine (albeit applied today in a more diverse society than the common-law societies from which they were derived), the explosion of digital technologies may have fractured privacy expectations such that a reasonableness determination captures little about *any* one individual's privacy expectations. For instance, young people, aware of digital information proliferation and accustomed to routine social media use, frequently see themselves as constant emitters of information and thus may not expect their personal information to be private.[66] Older individuals, who are often less conversant with—and less dependent on—the internet and computing, may expect that their information remains private in a manner analogous to nondigital forms of communication like physical mail.[67] Similarly, technology-minded individuals who understand the privacy-eroding potential of digital technologies may take steps to safeguard their data, thus indicating a desire for data privacy,[68] while others may take no such precautions.[69] Lumping all persons into a single "reasonable person" in the *Katz* analysis may fail to capture the actual privacy expectations of any portion of the population.[70]

Notwithstanding any shortcomings it may have, *Katz*'s descriptive reasonableness has remained the primary test for Fourth Amendment searches for nearly fifty years.[71] However, the explosion of information and communication technologies, with the resultant proliferation of data to third parties, has shocked the system. Mechanical application of existing

64. *See* Florida v. Riley, 488 U.S. 445, 451–52 (1989).

65. *See* Haley Plourde-Cole, *Back to* Katz*: Reasonable Expectation of Privacy in the Facebook Age*, 38 FORDHAM URB. L.J. 571, 580 (2010).

66. *See* Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1035, 1039–46 (2011); *see also* SYDNEY JONES & SUSANNAH FOX, PEW INTERNET PROJECT DATA MEMO: GENERATIONS ONLINE IN 2009, at 1–2 (2009), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2009/01/PI_2009.01.28_generations-online-in-2009_FINAL.pdf [https://perma.cc/5FYY-SM6X].

67. *See* Leary, *supra* note 66, at 1045 n.41.

68. *See Who Uses Tor?*, TORPROJECT.ORG, https://www.torproject.org/about/torusers.html.en [https://perma.cc/LLL4-RTS7]; *see also, e.g.*, Dell Cameron, *Edward Snowden Tells You What Encrypted Messaging Apps You Should Use*, DAILY DOT (Mar. 6, 2015, 10:11 AM), http://www.dailydot.com/politics/edward-snowden-signal-encryption-privacy-messaging [https://perma.cc/8HZ3-A79C].

69. *See* Craig E. Wills & Mihajlo Zeljkovic, *A Personalized Approach to Web Privacy—Awareness, Attitudes, and Actions*, 19 INFO. MGMT. & COMPUT. SEC. 53, 64 (2011).

70. *See The Fourth Amendment's Third Way*, 120 HARV. L. REV. 1627, 1635–36 (2007).

71. *See* Kevin Emas & Tamara Pallas, United States v. Jones*: Does* Katz *Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116, 125–40 (2012).

jurisprudence on reasonable privacy expectations and disclosure to third parties falters in the face of the unparalleled growth in surveillance capabilities enabled by expanding digital technologies. Cases involving observations taken from helicopters[72] or police officers surveilling houses through infrared cameras,[73] which were cutting-edge issues in their day, are not analogous to the scale, automation, and ease of modern surveillance.

B. *Cell Site Location Information*

Judge Wynn is attentive to these issues and has led the way in reformulating the third-party doctrine for the digital era. In *United States v. Graham*,[74] the en banc Fourth Circuit upheld law enforcement's warrantless collection of the defendant's cell site location information ("CSLI"), which it used to place him near the site of a robbery.[75] CSLI is data from cell phone towers, which register and log when a particular cell phone (or other cellular-enabled device) in the vicinity attempts to connect to them. Because cell phones attempt to connect to multiple towers in an area, the location of a particular phone—and the person carrying that phone—can be narrowed by reference to the towers that received the phone's signal.[76]

The court's reasoning was simple: the defendant, by using his cell phone, had voluntarily provided information that could identify his location—the phone's pings to nearby cellphone towers—to his cell service provider.[77] So, under the third-party doctrine, he could not claim any reasonable expectation of privacy in that data and could not claim that the police needed a warrant to obtain the data from the service provider.[78]

Judge Wynn dissented. Rather than beginning with the legal doctrine and working back to the facts, he began with a pragmatic example illustrating the realities of the situation:

> A customer buys a cell phone. She turns it on and puts it in her pocket. With those acts, says the majority, she has "voluntarily conveyed" an unbounded set of personal location data to her service provider, all of which is unprotected by the Fourth Amendment. Here, that included 221 days' worth of information, amounting to roughly 29,000 location-identifying data points . . . .[79]

72. *See* Florida v. Riley, 488 U.S. 445, 451 (1989).
73. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001).
74. 824 F.3d 421 (4th Cir. 2016).
75. *Id.* at 424.
76. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).
77. *Graham*, 824 F.3d at 427.
78. *Id.* at 425.
79. *Id.* at 441 (Wynn, J., dissenting).

To Judge Wynn, holding that this minimal activity "voluntarily conveyed" such a vast trove of information to a third party stretched the bounds of credulity. Conducting a detailed read of the Supreme Court's third-party doctrine decisions, he concluded that two elements were present in every case finding information voluntarily conveyed: first, that the defendant knew she was communicating particular information, and second, that the defendant took some affirmative action to submit that information.[80] In contrast, cell phone owners typically do not know that they are generating CSLI every moment their phone is on; nor are they aware that they are conveying such information to their phone provider and, upon request, law enforcement. Judge Wynn concluded that the Supreme Court never intended the third-party doctrine to cover the simple act of signing up for a phone line, thereby conveying thousands of pages of personal data.[81]

The Supreme Court later agreed with Judge Wynn. In *Carpenter v. United States*,[82] the Court held that an individual has a legitimate privacy interest in CSLI, and thus that the third-party doctrine does not excuse the need for law enforcement to obtain a warrant for such data.[83] In arriving at that conclusion, the Supreme Court articulated the same concerns as Judge Wynn in *Graham*. "[W]hile the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records."[84] At the time of the third-party doctrine's adoption, "few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[85]

The Supreme Court also adopted the arguments espoused by Judge Wynn in *Graham*: "Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term." Instead,

> a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. . . . As a result, in no meaningful sense does the user voluntarily "assume[] the risk" of turning over a comprehensive dossier of his physical movements.[86]

80. *Id.* at 443.
81. *Id.* at 446.
82. 138 S. Ct. 2206 (2018).
83. *Id.* at 2217.
84. *Id.* at 2216–17.
85. *Id.*
86. *Id.* at 2220.

Graham demonstrates Judge Wynn's sensitivity to technological erosion of Fourth Amendment protections and his willingness to stake out common-sense positions contrary to established doctrine on the basis of new factual scenarios.

C. *Cell Site Simulators*

Because Judge Wynn decides surveillance cases based on a hard look at the technical facts, he takes umbrage at government efforts to avoid disclosing the operational details of surveillance technology. This issue came to the fore in *Andrews v. Baltimore City Police Department*,[87] where the police used a cell-site simulator to locate the defendant.[88]

Cell-site simulators are devices that masquerade as cell phone towers.[89] Responding to signals emitted by the simulator, each cell phone and other cellular-enabled device in the simulator's vicinity identifies the simulator as the best local cell phone tower and transmits a connection signal containing that device's unique identifier to the simulator.[90] Because cell-site simulators are often handheld, police officers use them to monitor signal strength and direction while moving around an area to close in on the location of a particular cell phone.[91] That is what happened in *Andrews*—the police moved around within a crowded public housing block in Baltimore to pinpoint the defendant's cell phone inside one residence.[92]

The government conceded that the device searched the defendant's cell phone. Further, it did not dispute that the simulator was capable of reaching into homes and other constitutionally protected areas to determine which cell phones were inside—not unlike the infrared camera in *Kyllo*.[93] If sufficiently widespread, such searches could potentially violate the Fourth Amendment's requirement that a warrant specify with particularity the places to be searched and the items to be seized.

But the precise details of how broadly the simulator reached—its effective operational range, what data it gathered and from whom, and what measures it took to avoid collecting data from nonsuspect cell phones—were subject to a nondisclosure agreement between the government and the device's manufacturer.[94] The agreement prevented the government from disclosing, even to courts, how the device operated. Relying on the agreement, the

87. 8 F.4th 234 (4th Cir. 2020).

88. *Id.* at 235.

89. Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185 (2014).

90. DEP'T OF JUST., POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 2 (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/MCW2-R4QM].

91. *See* Owsley, *supra* note 89, at 193–94.

92. *Andrews*, 8 F.4th at 235.

93. Kyllo v. United States, 553 U.S. 27, 27 (2001).

94. *Andrews*, 8 F.4th at 235 n.1.

government refused to specify how many individuals' homes and phones were accessed as the police attempted to locate the defendant.

Demonstrating how he does not hesitate to use an analogy once he understands a technology on its own terms, Judge Wynn faulted the government, noting that the device's use was equivalent to a warrant allowing the police to open the door to every home in the simulator's operational range to determine if the defendant's phone was inside.[95] Such a broad warrant would lack particularity and plainly be forbidden as equivalent to the much-reviled "general warrants" used by the British that led the Founders to adopt the Fourth Amendment in the first place.[96]

Accordingly, Judge Wynn authored an order remanding the case to the district court to conduct discovery into the scope of constitutional intrusions enabled by the device, notwithstanding the nondisclosure agreement. This was one of the first orders of its kind because police departments have, as noted, gone so far as to dismiss criminal cases in order to avoid discovery into how broadly cell-site simulators reach.[97]

D. *Structural Disadvantages for Plaintiffs in the Surveillance Context*

In another case addressing government disclosure of surveillance capabilities, *Attkisson v. Holder*,[98] an investigative journalist alleged that unnamed U.S. government actors unlawfully conducted electronic surveillance on her internet-connected personal and work devices.[99] The panel majority dismissed the action, in part because it found the plaintiff did not identify any particular defendant with specificity.[100]

Judge Wynn dissented, noting that it was unsurprising that the plaintiff could not identify the defendants given the "profound information asymmetry" present when a plaintiff seeks to recover for unlawful government surveillance.[101] First, "the defendants nearly always have exclusive control over virtually all information necessary to identify the individuals responsible for engaging in allegedly unconstitutional or unlawful electronic surveillance."[102] Second, the defendants are often "protected by statutes and regulations preventing the disclosure of classified documents and programs as well as judicial orders sealing records related to warrants issued in criminal and national

95. Oral Argument at 35:03–35:10, *Andrews*, 8 F.4th 234 (No. 18-1953) [hereinafter *Andrews* Oral Argument], https://www.ca4.uscourts.gov/OAarchive/mp3/18-1953-20200128.mp3 [https://perma.cc/XJ7V-K55K].

96. *See* Pennsylvania v. Mimms, 434 U.S. 106, 109 (1977).

97. *See* United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, C.J., dissenting).

98. 925 F.3d 606 (4th Cir. 2019), *as amended* (June 10, 2019).

99. *Id.* at 620.

100. *Id.* at 627–28.

101. *Id.* at 642 (Wynn, J., dissenting).

102. *Id.*

security investigations."[103] Finally, "[t]he nature of the Internet, which allows wrongdoers to conceal their identity in a variety of ways, poses further obstacles to identifying individuals responsible for electronic surveillance."[104]

As in *Bosyk*, Judge Wynn chided his colleagues for failing to engage with the technology, stating that "courts must not avoid the difficult legal issues raised by new technology by erecting procedural barriers that ensure they never will be addressed."[105]

In *Attkisson*, as in *Andrews*, Judge Wynn's pragmatic, facts-based instincts were on display—he was alert to a significant legal issue arising from a novel technological situation but refused to decide it until he had all the facts on the technology. That focus continues to set him apart in this challenging and rapidly evolving area of the law.

V. ARTIFICIAL INTELLIGENCE AND PREDICTIVE POLICING

As a final note in the Fourth Amendment context, Judge Wynn has hesitated to trust the veneer of objectivity that often attaches to novel computerized police techniques. Most illustrative is *United States v. Curry*,[106] in which the en banc Fourth Circuit held that exigent circumstances did not justify a warrantless stop of the defendant, who was walking in a field near the location of gunshots in a public housing development categorized as a "high crime area" by the police.[107]

Writing in dissent, Judge Wilkinson lauded the use of "predictive" or "hot spot" policing techniques, noting that the "advent of big data and machine learning . . . [have] empowered officers to identify likely areas of crime with block-by-block precision," thus permitting focused police responses in areas of potentially high crime.[108]

In response, Judge Wynn first went to the scientific details, noting that many sources relied on by Judge Wilkinson did not provide any statistical analysis or empirical data linking reductions in crime to predictive techniques.[109] Judge Wynn then observed that "talismanic references to technological terms such as 'big data' and 'machine learning' should not be used as a screen for objectivity when analyzing the constitutional sufficiency of hot-spot policing programs and the law enforcement responses they enable."[110] Rather, predictive

103. *Id.*

104. *Id.*

105. *Id.* at 643.

106. 965 F.3d 313 (4th Cir. 2020).

107. *Id.* at 315–17.

108. *Id.* at 347 (Wilkinson, J., dissenting). To be clear, the issue in this case had nothing to do with big data and machine learning—dissents and concurrences, unlike majority opinions, often discuss topics only tangentially related to a case.

109. *Id.* at 334–35 (Wynn, J., concurring).

110. *Id.* at 336 n.1.

systems are only as good as the people who design them, feed them data, and interpret their results. Because the data provided to police systems already reflects various priorities and biases, a vicious cycle results: the system predicts more crime at locations where crimes have already occurred; the police focus their limited resources on those areas to stop additional crimes (while failing to detect crime in other areas due to resource constraints); and the resulting crime data is fed back into the predictive system, which predicts even further crime in the "hot spot" areas.[111] As Judge Wynn noted, "[such] predictive algorithms may only potentially confirm (or reinforce) what the police already know (or believe) about where crime is occurring."[112]

CONCLUSION

Judge Wynn's pragmatic, facts-first jurisprudence is well suited to disputes involving technology, which often involve issues of first impression not readily addressed by analogy to existing precedent.

Such flexible, case-by-case determination is appropriate for a period of rapid technological growth, given that legislative action addressing emerging technology has historically been slow and that prospective rules may apply for only a short time before technology moves past them. Judge Wynn noted as much in the *Andrews* case, stating that although the specific issue before the court was use of a cell-site simulator, neither "this Court nor any court can ignore the changing technology, because if we do, we might as well throw the Fourth Amendment out of the window."[113] He further noted that, in light of law enforcement's willingness to use ever-broader and more intrusive means of technological surveillance, the courts "are the only thing that's between citizens and tyranny in this country."[114] Judge Wynn's colleague, Judge Wilkinson, wryly noted his concerns as "quite a parade of horribles" and accused him of generally exclaiming that "the sky is falling."[115] Thanks to his deep familiarity with the evolving technological landscape, Judge Wynn could confidently offer a simple response: "Indeed it is."[116] To that, he could have added: "and I'm going to do something about it."

111. *See* Joh, *supra* note 4, at 300–01.
112. *Curry*, 965 F.3d at 336 n.1 (Wynn, J., concurring).
113. *Andrews* Oral Argument, *supra* note 95, at 35:03–35:10.
114. *Id.* at 56:40–56:46.
115. *Id.* at 57:17–57:19.
116. *Id.* at 57:49–58:00.