A NEW STATE CONSTITUTIONAL RIGHT TO INFORMATION PRIVACY: THE ORIGINS SPEAK

Albert Scherr

Neal Kurk[†]

ABSTRACT

When the Supreme Court issued its sweeping decision in *Dobbs v. Jackson Women's Health Organization*,[1] it sent the fate of abortion rights to the states and in turn, brought renewed focus to state constitutional rights. In its *Dobbs* opinion, the Court's majority made abundantly clear that it is interested in reconsidering several landmark decisions related to civil rights. This has ignited discussion about how state constitutions could potentially step up to fill the void that the

† Albert Scherr is a Professor of Law at UNH School of Law and a New Hampshire State Representative. Representative Neal Kurk is a retired state representative in the New Hampshire House of Representatives. Professor Scherr and Republican Representative Kurk (now retired) were the drafters of Part I, Article 2b and Representative Kurk was the prime sponsor of the constitutional amendment (CACR 16) that became Article 2b. Thanks to Jeanne Hruska for her editorial prowess.

1. Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

Supreme Court is in the midst of creating when it comes to federal constitutional rights.

This heightened interest in state constitutions is not without merit. Over the decades, many states have developed stronger civil rights protections than those provided by the U.S. Constitution. This has been achieved through a combination of constitutional amendments and state court jurisprudence.[2] There are states that have gone in the reverse direction, cutting back on civil rights protections, making the U.S. Constitution more of a ceiling than a floor in those respective states.[3] This feeds into the notion of state courts and constitutions as a laboratory for experiments in constitutional law.[4] Put differently, state bills of rights have been viewed as "ordinance(s) of the people."[5] Or, amplifying that idea: "a dynamic set of substantive instructions and limitations on government that is adopted and jealously maintained by the people themselves."[6]

Lawyers across the country have begun to put their respective state constitutions under a more powerful microscope. The *Dobbs* Court noted that the word "abortion" does not appear in the U.S. Constitution[7] The word "privacy" also does not appear in the U.S. constitution; however, it does appear in a number of state constitutions.[8] And while the U.S. Supreme Court increasingly has been skeptical of the expanse of the Fourth Amendment's privacy protections, state courts have taken differing approaches to their own state constitution's privacy protections.

This article occupies the space between the ongoing, newly energized development of state constitutional law and the fraught public

2. One can find a partial survey of such cases in ROBERT F. WILLIAMS, THE LAW OF AMERICAN STATE CONSTITUTIONS 119–27 (2d ed. 2009). For example, the New Hampshire Supreme Court has developed a robust body of law over the past several decades more protective of criminal defendants' rights under the New Hampshire State Constitution. *See, e.g.*, State v. Phinney, 370 A.2d 1153, 1154 (N.H. 1977); State v. Settle, 447 A.2d 1284, 1286 (N.H. 1982); State v. Ball, 471 A.2d 347, 351–53 (N.H. 1983); State v. Canelo, 653 A.2d 1097, 1105 (N.H. 1995); State v. Bushey, 453 A.2d 1265, 1267–68 (N.H. 1982); State v. Goss, 834 A.2d 316 (N.H. 2003).

3. *See* Jonathan L. Marshfield, *America's Misunderstood Constitutional Rights*, 170 U. PA. L. REV. 853, 869–70 (2022).

4. *See* JEFFREY S. SUTTON, WHO DECIDES? STATES AS LABORATORIES OF CONSTITUTIONAL EXPERIMENTATION (2022).

5. Wesley W. Horton, *Annotated Debates of the 1818 Constitutional Convention*, 65 CONN. BAR J. 3, 17 (1991).

6. Marshfield, *supra* note 3, at 859–60.

7. Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 225 (2022).

8. *See infra* Part II(B)(2).

policy field of privacy protections. It analyzes a new state constitutional provision that is explicitly and exclusively about information privacy. The provision, Part I, Article 2b[9] of the New Hampshire Constitution,[10] reads as follows:

> *An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent.*[11]

The provision extends an individual's privacy right significantly beyond that of both the federal and New Hampshire state constitutions. It operates at the intersection of privacy and of 21st century technology, state and federal constitutional law and jurisprudence, as well as state and federal laws and regulations. Historically, the mix of law addressing this challenging intersection was primarily a patchwork quilt that tended to favor technology over privacy.

Article 2b is a model for prioritizing privacy in this digital age. As its history reflects, it is both a 21st century "ordinance of the people" and "a dynamic set of substantive instructions and limitations on government that is adopted and jealously maintained by the people themselves."[12] Analysis of that ordinance of the people is the goal of this article. While Article 2b was enacted in 2018, four years before *Dobbs*, it is all the more relevant in a post-*Dobbs* world when lawyers and the public will increasingly turn to state constitutions to protect themselves from the prying eye of government, or the even more invasive eye of Big Tech.

INTRODUCTION

When the Framers of our 18th century federal constitution wrote the amendments that came to constitute the Bill of Rights, privacy was about one's physical possessions and dwelling. In the 21st Century, privacy is also about our personal information. The problem: 18th century law was not written for 21st century information privacy. Needless to say, defending privacy rights in the 21st century with 18th century law is often a losing battle. One need only look at Big Tech's infiltration of the barriers to collecting our personal and private data to understand this.

---

9. *Hereinafter,* Article 2b.
10. N.H. CONST. pt. I, art. 2-b (2018) [hereinafter Article 2b].
11. *Id.* (emphasis added).
12. Marshfield, *supra* note 3, at 859–60.

Part of this problem is that 21st century technology has exponentially expanded the ways that our personal data can be—and is—accessed, collected, consolidated and analyzed, often without notice or permission. Some of those ways have simplified access to previously biologically locked data, like relatively routine access to genetic information.[13] Some have turned that which was previously not regarded as data[14] into accessible data, like facial recognition's technology rendering of human faces into accessible data points.[15] Some of it has amassed previously scattered, difficult-to-collect data into revealing mosaics of data, like GPS technology's collection of public-whereabouts data.[16] More broadly, information is being accessed and collected into innumerable types of databases. Private and public medical research often create databases with a wealth of personal information beyond genetic "types." Cellphone and internet providers act as repositories for vast amounts of geo-locational information; cellphone behavior and internet activity. Private businesses not infrequently have security cameras for their establishments and retain the videos. Larger businesses collect vast amounts of data about customer behavior that they both store and sell. Only some of the above occurred during most of the 20th century, let alone the 18th century.

The federal constitution's focus is directly on the container or location of information. The Fourth Amendment speaks of "persons, houses, papers, and effects" as does Part I, Art. 19 of the New Hampshire Constitution.[17] It misses the mark in the 21st century when privacy is about the information itself, which in digital form can be readily transferable, multiplied, and shared. The product of 21st century technology—information—exists independent of physical location, be it geographically, or in a container. By contrast, in the 18th century, information existed in containers and in some physical form (with the

13. *See* Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445, 447 (2013).

14. We use the terms "data" and "information" interchangeably in this essay.

15. *See* Kashmir Hill, *New Jersey Bars Police From Using Clearview Facial Recognition App*, N.Y. TIMES (Jan 24, 2020, 5:39 PM), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html?searchResultPosition=4; Alan Rappeport & Kashmir Hill, *I.R.S. to End Use of Facial Recognition for Identity Verification*, N.Y. TIMES (Feb 7, 2022, 12:45 PM), https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html?searchResultPosition=9; Sahil Chinoy, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019, 10:11 AM) https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html?searchResultPosition=15.

16. *See, e.g.,* U.S. v. Jones, 565 U.S. 400 (2012).

17. U.S. CONST. amend. IV; *see* N.H. CONST. pt. I, art. 19.

exception of information contained in one's thoughts, which was addressed by the right against self-incrimination in the Fifth Amendment). Though, arguably, the essence of Art. 19's and the Fourth Amendment's focus on containers is to protect the information contained therein, their language does so indirectly, at best.

Fourth Amendment jurisprudence has long sought to address this discrepancy between the 18th and 21st century challenges to privacy and the changing nature of the information through the "reasonable-expectation-of-privacy" standard from *Katz v. United States*.[18] *Katz,* taking place in 1967, involved information in the form of one end of a two-way conversation occurring in what would now be considered an old-fashioned a traditional phonebooth,[19] and yet even such an old-fashioned setting could not have been a circumstance anticipated by the drafters of the Fourth Amendment. *Katz* recognized that what merited privacy with regards to the conversation in question was the content of the relevant phone conversation in that phonebooth in which the speaker had shown an expectation of privacy, an expectation the court also decided was worthy of societal recognition. While location was still important to that decision, the court was beginning to analytically distinguish information from its container.

This analytical change continued in fits and starts over the next few decades in Supreme Court cases like *Kyllo v. United States* (reasonable expectation of privacy in potentially intimate information from the inside of a house gained without even entering the house using a thermal imaging device on public property)[20] and *California v. Greenwood* (no reasonable expectation of privacy in contents of garbage bag left at end of driveway for collection).[21] The Court was balancing the nature of the container, the nature of the information in that container and the nature of the circumstances in applying the reasonable-expectation-of-privacy standard.

The *Katz* standard provided a lot of flexibility and discretion for the courts, for better and for worse. This resulted in the outcome being very much dependent on a judge's own sense of "privacy." For example, a number of state courts have come out differently on the "garbage" question of whether someone has a "reasonable expectation of privacy" to their garbage under their state constitutions. New

18. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
19. *Id.* at 353–54.
20. *See* Kyllo v. United States, 533 U.S. 27, 34–35 (2001).
21. *See* California v. Greenwood, 486 U.S. 35, 41 (1988).

Hampshire, New Jersey, Iowa, Washington and others have found a reasonable expectation of privacy in the contents of a garbage bag.[22]Each of these courts effectively had a difference of opinion with the Supreme Court over whether a reasonable expectation of privacy existed in the "papers and effects" in garbage or in the "information" in garbage.

As we've moved further into the 21st century, our lives are increasingly lived online and our most private information increasingly digitized. The Supreme Court's struggle to establish clear and consistent jurisprudence using the reasonable-expectation-of-privacy standard has faltered. In *United States v. Jones*,[23] for example, the police put a GPS tracking device on the underside of Jones's SUV while it was parked in a public space. They then used the device to track his whereabouts over several days, gathering a wealth of data from this surveillance. The government contended that such tracking did not constitute a search as the police had not entered Jones's SUV and they had merely acquired otherwise publicly available data[24]

What is interesting about the Court's 9-0 opinion concluding that the surveillance constituted a search within the meaning of the Fourth Amendment is not the outcome. It is the three different opinions that aspire to place the use of this particular 21st century technology within the Court's now somewhat outdated Fourth Amendment jurisprudence. Four justices centered their analysis on a property paradigm, using 18th century tort law to characterize the placement of the GPS on the SUV as a trespass. One judge agreed that the property paradigm was a minimum starting point for a Fourth Amendment analysis but ultimately relied more heavily on an expansive reasonable-expectation-of-privacy analytical framework, focusing on the breadth of the information collected.[25] Finally, four other judges acknowledged that the property-paradigm and reasonable-expectation-of-privacy approaches each had deficiencies in light of technological developments. They relied on a far more restrained reasonable-expectation-of-privacy analysis to agree on the outcome in this particular case with no

22. *See, e.g.*, State v. Goss, 834 A.2d 316, 319 (N.H. 2003); State v. Hempele, 576 A.2d 793, 810 (N.J. 1990); State v. Wright, 961 N.W.2d 396, 418–19 (Iowa 2021); State v. Boland, 800 P.2d 1112, 1116 (Wash. 1990).

23. *See* United States v. Jones, 565 U.S. 400 (2012).

24. *Id.* at 402–03.

25. *See id.* at 954–57 (Sotomayor, J., concurring).

predictions as to future outcomes regarding new surveillance technology.[26]

A recent and more telling example of the jurisprudential struggle over 21st century technology's intersection with the Fourth Amendment is *Carpenter v. United States*.[27] There, the Court considered whether records of cell-site location information (CSLI) were protected by the Fourth Amendment.[28] Interestingly, such information was a 21st century version of data akin to 20th century telephonic pen registers. In *Smith v. Maryland* and *United States v. Miller*, the Court applied the third-party doctrine to pen registers and bank records, respectively, in finding that an individual has a reduced expectation of privacy in information knowingly shared with another and considering the nature and content of the documents at issue. In those circumstances the individual thereby had no Fourth Amendment protection.[29]

In *Carpenter,* the Court dodged whether to abandon the third-party doctrine. Instead, it focused on the breadth and extent of the information collected from "12,898 location points cataloging Carpenter's movements over 127 days."[30] It was a 5-4 decision with four separate dissents. The majority distinguished their holding from *Smith v. Maryland* and *U.S. v. Miller* not by abandoning the third-party doctrine, but by focusing on the more comprehensive nature of the information gathered.

One dissent captured the sentiment of all four dissents well in criticizing the majority opinion as a "stark departure" from *Smith* and *Miller*[31] Combined, the four dissents took the majority opinion to task for its mistaken reliance on the reasonable-expectation-of-privacy standard; for fracturing two fundamental pillars of Fourth Amendment law; and for failing to harken back to the text and original understanding of the Fourth Amendment. The variety of approaches in the majority and the dissents reflected the serious jurisprudential struggle in applying the Fourth Amendment, and the Court's own container/location dependent precedent, to 21st century technology.

---

26. *See id.* at 957–64 (Alito, J., Ginsburg, J., Breyer, J., & Kagan, J., concurring).

27. *See* Carpenter v. United States, 585 U.S. 296 (2018).

28. *See id.* at 300.

29. *See* Smith v. Maryland, 442 U.S. 735, 744–45 (1976); United States v. Miller, 425 U.S. 435, 442 (1979).

30. *See Carpenter*, 585 U.S. at 296.

31. *Id.* at 321 (Kennedy, J., Thomas, J., & Alito, J., dissenting)

The Court's jurisprudential struggle also produced noteworthy inconsistencies in a broader context. For example, in *Riley v. California*,[32] the police gained possession of Riley's cellphone through a search incident to arrest and proceeded to search the contents of the phone without obtaining a search warrant. The Court's ruling required the police to get a search warrant in such circumstances, given the nature of the digital information in a cell phone. The Court emphasized the potential multi-dimensional nature of the digital data: that it had vast storage capacity for a variety of texts, videos and pictures; that it could have data dating back several years; and that it contained a digital record of nearly every aspect of a person's life.[33]

The opinion is noteworthy here for three reasons. First, it was a unanimous opinion on what is perhaps the classic representation of 21st century technology, a smartphone. Second, Justice Alito in his concurrence explicitly referred to the Court's ongoing challenge with new technology:

> I agree that we should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests.[34]

Third, the Court's decision, which focused on the nature and extent of the *digital* information in a cellphone, stands in stark contrast to a sequence of decisions by lower courts regarding *genetic* information in surreptitious DNA harvesting cases. This developing potential conflict again reflects that the Court's 20th century jurisprudence was a bad fit for much 21st century technology. In one such case, the police developed a genetic profile of a crime scene sample of unknown origin. Though they had a suspect, they did not have probable cause for a search warrant to get saliva or blood from the suspect so they could generate their genetic profile for comparison. Instead, the police acquire the necessary bodily fluid surreptitiously from the suspect, be it from the back of a stamp or an envelope on returned mail,[35] from a

32. *See* Riley v. California, 573 U.S. 373, 378–79 (2014).
33. *See id.* at 393–95.
34. *Id.* at 406–07 (Alito, J., concurring).
35. *See* State v. Athan, 158 P.3d 27, 32 (Wash. 2007).

cigarette butt, or from a soda can offered to the suspect in a non-custodial interview at the police station.[36]

By contrast, virtually every court, state and federal, has found that surreptitious DNA harvesting does not implicate Fourth Amendment interests though, in concept, a cell phone containing personal information is essentially identical to a biological cell containing personal information. Most often, courts rely on some version of a property-based analysis: the suspect abandoned the stamp, the coffee cup, or the cigarette butt voluntarily and, thereby, relinquished a Fourth Amendment interest in their DNA.[37] Ironically, in 2014, the Supreme Court found that the *digital* contents of one kind of cell (a cell phone) merited Fourth Amendment protection[38] but, in 2015, declined certiorari in a case in which the Maryland Court of Appeals did not give Fourth Amendment protection to the *genetic* contents of another kind of cell (the cells in the saliva in a soda can left by the suspect at a police station).[39]

Courts' indirect distinction between digital cell content and biological cell content presages a likely ongoing jurisprudential struggle with 21st century technology. It may well be that a thoughtful distinction exists between the reasonable expectation of privacy in the digital information in a cell phone and the genetic information within a biological cell. For example, genetic information in a cell is much more profoundly locked up, through a number of not easily unlocked biological barriers, than is digital information. Additionally, people are generally more cognizant of the private nature of certain cell phone content (pictures, lurid texts, passwords, etc.) than they are of their DNA. But, the prism of the Fourth Amendment has substantially muddled and sidetracked this important discussion about 21st century technology with too much attention to property and container-based analogies and analysis. Part I, Article 2b clears up that muddle for New Hampshire.

I. PART I, ARTICLE 2B[40]

If we look to literature, it is nearly impossible to find a common understanding of privacy other than perhaps the notion that context

36. *See* Scherr, *supra* note 13, at 450–51.

37. *See id.* at 454–58.

38. *See* Riley v. California, 573 U.S. 373, 403 (2014).

39. *See* Raynor v. State, 99 A.3d 753 (Md. 2014) (emphasis added).

40. Part II represents a comprehensive description of the intent of Professor Scherr and Representative Kurk when they drafted Part I, Article 2b. Rather than

matters.[41] Privacy itself is a multi-dimensional, personal, and often amorphous concept that has meant many different things to many different people. Many of the conceptions relate to information and control of information. Daniel Solove has suggested a number of different conceptions that frequent legal and philosophical discourses about privacy:

> (1) the right to be let alone—Samuel Warren and Louis Brandeis's famous formulation of the right to privacy; (2) limited access to the self—the ability to shield oneself from unwanted access by others; (3) secrecy—the concealment of certain matters from others; (4) control over personal information—the ability to exercise control over information about oneself; (5) personhood—the protection of one's personality, individuality, and dignity; and (6) intimacy—control over, or limited access to, one's intimate relationships or aspects of life.[42]

The protection of information from government intrusion is only a part of privacy. For example, the mere presence of the government in one's life, with or without the knowledge of the individual, is itself often viewed as a separate "dignitary" privacy violation, regardless of what the government does with that presence. But, it is an essential part and has been bogged down by the various Fourth Amendment iterations of the property paradigm, by the reasonable-expectation-of-privacy debate, and by 18th century property and tort law.

Solove's list reflects much of the essence of what bothers people in the 21st century about governmental intrusions or, for that matter, commercial intrusions. Particularly with modern technology, so much of one's identity is captured in personal information: medical, genetic, financial, political, biometric, social etc. Privacy in personal information has taken on a heightened importance amidst the explosion of tools for harvesting personal information. The instincts remain the

---

repeat in each sub-section of Part II that the description therein reflects the intent of the drafters, the reader should understand with certainty that Part II accurately describes the intent of the drafters of Article 2b.

41. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (arguing that privacy must be seen in a social context); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 12–13 (2008).

42. *See* SOLOVE, *supra* note 41, at 12–13. Solove argues persuasively that none of these conceptions capture the common denominator of privacy. *Id.* at 14. He goes on to propose a "taxonomy of privacy" that seeks to provide a better understanding of privacy. *Id.* at 101–02.

same: "Stay out of my personal information unless I consent to let you in. It's mine and not the government's to control."

Part I, Article 2b of the New Hampshire Constitution honors these instincts for notice, consent, and control by constitutionalizing them. It frees 21st century technology from the unwieldy property paradigm of 18th century privacy. Article 2b places information—also known as data when digitized—at the core of the analysis, a shift that is meaningful in practice while still honoring the deep meaning of constitutional privacy under Part I, Article 19 of the New Hampshire Constitution or the Fourth Amendment of the U.S. Constitution because it addresses directly that which underlies each of those amendments: the privacy of information.

Article 2b modernizes the constitutional protection of information sought by the New Hampshire government. That is its point and its effect. As one witness before the Senate Rules and Enrolled Bills Committee said in her written testimony:

> New Hampshire never had a need to address information privacy protection until the late 20th and early 21st Century. Before then, statutory protection and the state's libertarian spirit were by and large adequate to manage the occurrences of intrusions on personal information and data. That is no longer true. The onslaught of governmental and commercial intrusions into our informational privacy is an overwhelming and unstoppable tide. Increasingly, our statutory protections are more patchwork than comprehensive as the potential intrusions diversify and multiply. This CACR would remedy that for New Hampshire by enshrining in our state constitution a specific right to governmental non-interference in which our state firmly believes.[43]

It does this by shedding the overwrought concerns about locations and containers. At best, locations and containers of information may, in some cases, add some secondary or tertiary meaning under Article 2b as to whether the information is personal or private, but that is all. It renders irrelevant considerations of 18th century property and tort law.

---

43. *Constitutional Amendment Concurrent Resolution 16: Hearing on 2018-1936e Before the Senate Rules and Enrolled Bills Committee*, 2018 (N.H. 2018) (written testimony of Jeanne Hruska, Policy Director, ACLU-NH).

Article 2b's legislative history reflects this shift. The exchange between Senator Kevin Avard and Representative Renny Cushing at the Senate Rules and Enrolled Bills Committee Hearing reflects the importance of then CACR 16:

> **Representative Cushing** introduced the bill. "The essence of liberty is the right to be left alone. This amendment will clarify that liberty includes the right to privacy."
>
> **Senator Avard** – "I thought this was already assumed?"
>
> **Representative Cushing** – "As technology evolves over time and because privacy is the essence of liberty, this makes it more explicit."[44]

A further exchange between Senator Avard and Representative Dan McGuire on the NH Liberty Alliance reinforced how Article 2b marks the change in focus from location to information:

> **Senator Avard** – "Would this prevent the government from seeking out that information from third parties?"
>
> **Representative McGuire** – "Yes, because it is about the individual's information, it doesn't matter where it is."[45]

Article 2b comprises unique state constitutional provisions that address privacy directly. Ten states have constitutional provisions that use the word "privacy" in some way.[46] Some invest an individual with a general "right to privacy."[47] Some prohibit "invasions of privacy."[48] Some protect "private affairs" or "private life."[49] One also directly

---

44. *Constitutional Amendment Concurrent Resolution 16: Hearing on 2018-1936e Before the Senate Rules and Enrolled Bills Committee*, 2018 (N.H. 2018) (testimony of Sen. Kevin Avard and Rep. Renny Cushing).

45. *Constitutional Amendment Concurrent Resolution 16: Hearing on 2018-1936e Before the Senate Rules and Enrolled Bills Committee*, 2018 (N.H. 2018) (testimony of Sen. Kevin Avard and Rep. Dan McGuire).

46. *See* ALASKA CONST. art. 1, § 22; *see also* ARIZ. CONST. art. 2, § 8; CAL. CONST. art. 1, § 1; FLA. CONST. art. 1, § 23; HAW. CONST. art. 1, § 6; ILL. CONST. art. 1, § 6; LA. CONST. art. 1, § 5; MONT. CONST. art. 2, § 10; S.C. CONST. art. 1, § 10; WASH. CONST. art. 1, § 7.

47. ALASKA CONST. art. 1, § 22; *see* CAL. CONST. art. 1, § 1; *see also* HAW. CONST. art. 1, § 6; MONT. CONST. art. 2, § 10.

48. ILL. CONST. art. 1, § 6; *see* LA. CONST. art. 1, § 5; *see also* S.C. CONST. art. 1, § 10.

49. ARIZ. CONST. art. 2, § 8; *see* FLA. CONST. art. 1, § 23; *see also* WASH. CONST. art. 1, § 7.

protects "interceptions of communications by eavesdropping devices or other means."[50]

Article 2b is the only state constitutional provision that focuses explicitly and directly on information and intrusions on "personal or private" information rather than on privacy more broadly. And this focus is intentional. The provision specifically addresses the realities of 21st Century privacy, namely by focusing specifically and exclusively on and to address government intrusions on information. Thus, the goal was to switch the legal analysis from "which locations or containers" and "what counts as private" to "what intrusions" and "which information is personal or private?"

II. THE LANGUAGE OF PART 1, ARTICLE 2B

A. "Governmental Intrusion"

The consideration of whether governmental conduct is an intrusion on an individual's personal or private information is different than the Part I, Article 19 consideration of whether a governmental search is an intrusion on "his person, his houses, his papers, and all his possessions."[51] "Governmental intrusion" is intended to contemplate (1) observation of the defined ("personal or private") information, wherever it is located; (2) the collection of the defined information, however collected; (3) the retention of the defined information, however retained; and (4) the use of the defined information, however used.

(1) The mere *observation* of personal or private information is as a governmental intrusion under Article 2b, whether the governmental intruder goes on to collect, retain or otherwise use the information or not. This is due to the realities of 21st century information, whereby it is not only the possession of it that is intrusive, it's the mere observation of it. Think of a digital photograph, or the information on an electronic medical record. As soon as the government observes that

50. ILL. CONST. art. 1, § 6.

51. N.H. CONST. pt. 1, art. 19 (stating "[e]very subject hath a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. Therefore, all warrants to search suspected places, or arrest a person for examination or trial in prosecutions for criminal matters, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order, in a warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued; but in cases and with the formalities, prescribed by law.") [hereinafter Article 19].

information, it has intruded on the respective person's privacy, regardless of whether the government goes on to collect or retain the information in digital or physical form. For example, if a police officer views of information, irrespective of location, is an intrusion. It may be that the information does not have to meet the definition of "personal and private" information or that it survives a strict scrutiny analysis to trigger Article 2b. The observation in and of itself was intended by the drafters to count as an intrusion.

(2) The *collection* of personal or private information is also a governmental intrusion under Article 2b. For example, it does not matter whether the governmental collector goes on to use the particular personal or private information they collected or not. The collection, in and of itself, violates the provisions of Article 2b. That the government collects one's personal or private information, whether they use it or not. offends the protection provided by the amendment. As a result, the creation of a database, whether for current or future use, is prohibited under Article 2b unless the information collected is not personal or private or there is consent. For example, the collection by the government of digital representations of people's faces, an important piece of facial recognition technology, represents the collection of information. Depending on the circumstances, it may or may not survive an Article 2b analysis.[52]

(3) The *retention* of the defined information is also an intrusion under Article 2b. 2b intentionally does not allow the government to retain personal or private information even if it was collected consensually and even if it is never used. Very often, the collection may be consensual but, if the retention goes beyond the bounds of the specific and explicit consent given, it is prohibited by Article 2b.

For example, police may collect a biological sample from the victim of a sexual assault for purposes of creating a genetic profile to compare to the genetic profiles within the biological sample taken vaginally from the victim. Under Article 2b, they may not retain the victim's genetic profile in any statutory or other database or in any other way once they have used it for the consented-to purpose. As recent events reveal, this is not a hypothetical example.[53]

---

52. A digital representation of someone's face may have been placed in a location by that person after they explicitly read and signed a consent form.

53. *See* Azi Paybarah, *Victim's Rape Kit Was Used to Identify Her as a Suspect in Another Case*, N.Y. TIMES (Feb. 15, 2022), https://www.nytimes.com/2022/02/15/us/san-francisco-police-rape-kit-dna.html. "[T]he San Francisco Police Department identified a woman who was recently arrested on a felony

(4) The *use* of personal or private information is also an intrusion under Article 2b. Note that, in many instances, use of the defined information will have been preceded by either observation, collection or retention of the information. However, it may be that the defined information was observed, collected and/or retained with the consent of the individual whose personal or private information it is. From an Article 2b perspective, unless that individual has also consented to its use and the specific use in question the use of the information constitutes a governmental intrusion.

B. "Personal or Private Information"

The crux of Article 2b is understanding what is meant by "personal or private information." The unmodified definition of information is immensely broad. One need only look at the terms used by Webster's Dictionary:

> knowledge obtained from investigation, study, or instruction; intelligence; news; facts, data . . . a signal or character (as in a communication system or computer) representing data; something (such as a message, experimental data, or a picture) which justifies change in a construct (such as a plan or theory) that represents physical or mental experience or another construct, [etc] . . . .[54]

The two modifiers in Article 2b narrow that broad scope down but they remain quite expansive in order to give the leeway necessary in the twenty-first century when technology is constantly expanding the types and uses of information.

The legislative history of Article 2b reflects the intended breadth of the provision. In his Statement of Intent to the full House of

---

property crime charge based on DNA samples that she had given earlier when she reported that she had been sexually assaulted. Her DNA had been collected by investigators in order to identify her attacker." *Id.* The practice of using DNA from a rape kit to possibly identify the victim as a potential suspect in another matter is apparently widespread…" *Id.* Rachel Marshall, a spokeswoman for the district attorney's office, "said that using DNA from rape kits in this way might date back to 2015, when crime databases in the region were revamped." *Id.* She "said in an email on Wednesday that the office had dropped charges in the case, citing a violation of the Fourth Amendment, which protects people from unreasonable searches and seizures by the government." *Id.*

54. *Information*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/information (last visited Mar. 14, 2025).

Representatives on behalf of the House Judiciary Committee, Representative Kurt Wuelper wrote:

> CACR 16 formally recognizes our right to privacy in our personal information. We've long protected our privacy in our "person, houses, papers and effects", but this omits the modern ability to collect/analyze personal information, things like health data, information from our DNA, etc. Our personal information, today, is perhaps more important than those items already protected, and CACR 16 will provide the same protection to our personal data that we have for our physical things.[55]

During the Senate hearing on then CACR 16, Senator Bradley said:

> When I read this language and I see information, you may think that is digital but one's personal, medical history is also information. I think you are enshrining that right of your personal medical information into the constitution.[56]

Dan McGuire of the NH Liberty Alliance spoke in support of CACR 16 at that same hearing and gave an example:

> When the 4th amendment was adopted and section 19 of our constitution was put in physical private things was located somewhere papers, notes etc. They were visible to the eye. This constitutional provision is updating that kind of provision but for the modern world where there is a lot of information about people and it is not visible. Also things like your DNA, if you go to Starbucks and drink a cup of coffee and throw away that cup, it has your DNA on it. The police could pick that cup up and no search warrant is needed.[57]

1. "personal information"

As to the scope of protection of information, the language of Article 2b is much broader than the protection offered by Part I, Art. 19

55. H.R. COMM. REP. ON CACR 16, 2018 Sess. (N.H. 2018) (the proposal that became Part I, Article 2b passing with a vote of 15-2).

56. *Bill as Amended: Hearing on CACR 16 Before the S. Rules & Enrolled B. Comm.*, 2018 Sess. 2 (2018) (statement of Sen. Bradley, Member, S. Rules & Enrolled B. Comm.).

57. *Bill as Amended: Hearing on CACR 16 Before the S. Rules & Enrolled B. Comm.*, 2018 Sess. 2 (2018) (statement of Dan McGuire, Rep. of NH Liberty All.).

or the Fourth Amendment. After all, the very purpose of Article 2b is to provide privacy protections in the 21st century not currently provided by Article 19 or even by the Fourth Amendment, as it has been interpreted by the Supreme Court. As noted above, Article 19 and Fourth Amendment in the first instance offer protection for information based primarily on where it is located or in what it is contained. In the last sixty years, that protection was further refined to include protection for searches that invaded a reasonable expectation of privacy. And so, the inquiry has become whether the search invaded this kind of property or this sense of privacy. That inquiry has become more challenging with 21st century technology, which has dramatically expanded the means and goals of searches.[58]

Article 2b takes a different approach. It identifies the information itself as the primary focus. Definitions of personal information like those of the National Institute for Science & Technology (NIST) and the General Data Protection Regulations (GDPR) in Europe were considered. Both are internationally recognized and well-accepted definitions.

The NIST definition:

> Personally Identifiable Information (PII): any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[59]

This definition is expansive as compared to that which might be covered by any reasonable-expectation-of-privacy analysis. It includes biometric records such as genetic information, digital representations of faces, eye scans, etc. It also includes school records, medical records and the like; information that may already be protected to some extent by statute but will now have constitutional protection.

---

58. Consider, for example, the issues surrounding privacy in public. *See* PRIVACY IN PUBLIC SPACE: REGULATORY AND LEGAL CHALLENGES (Tjerk Timan, Bryce C. Newell & Bert-Jaap Koops eds., 2017).

59. ERIKA MCCALLISTER, TIM GRANCE & KAREN SCARFONE, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII), NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, at 2-1 (2010).

The GDPR provides an even more detailed set of definitions:

> '[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[60]

Article 9 of the GDPR drills down even more specifically with regard to certain types of data:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[61]

Article 9 data, commonly referred to as sensitive personal data, gets particularly strong protection under the GDPR.[62] The term "personal information" is intended to have this kind of broad meaning because the nature of 21st century technology is to develop more and more types of information and, even more importantly, more and more ways to observe, collect, store and use that information. These new types of information and methods for accessing information were unknown in previous centuries and some are still only creatures of the imagination even today.

An obvious example, as Shoshanna Zuboff details in her magisterial book, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, is the ability of tech companies like Google, Facebook and Amazon to collect vast amounts of

60. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 33 (EU) [hereinafter GDPR]. Note that while these definitions identified here did not go into formal effect until May 2018, the language quoted here had been available at the time of the drafting of Article 2b.

61. GDPR, art. 9(1).

62. *See id.*

data about specific individuals.[63] As another modern and increasingly common example, one private company has collected massive collections of digital representations of people's faces into a database that it sells to governments for identification purposes.[64]

More generally, personal information will include common-place data like records of: books withdrawn from the library; shows ordered on Netflix, Amazon Prime, Hulu etc.: commercial transactions; Venmo transactions; financial transactions; whether one voted; for whom one voted; political contributions; social media conversations; data generated by one's car; geo-location data; personal medical data; other private political activity; phone conversations; e-conversations and other digital information.[65]

The purpose of Article 2b's foundational principle was for privacy rights to stop playing catch up with technology and instead to build a right to privacy that could endure generations of technology not yet developed. To accomplish that purpose, Article 2b takes a very different approach to the kind of intrusion on personal information than currently existed under the New Hampshire Constitution, therein the expansive use of the term "personal information," which lies at the core of the foundational principle.

2. "or private information"

It may be that some information is not, on its face, personal but, nonetheless, has been deemed private by a statute, regulation or other mechanism, given the particular circumstances in which that information exists.[66] That kind of information is also protected by Article 2b. Notably, under Article 2b, personal information need not be private and private information need not be personal. Article 2b does not anticipate every possible circumstance in which information may exist and be subject to intrusion. Instead, the goal was to lay down a foundational principle tailored to the 21st century and beyond.

---

63. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

64. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

65. If the entity with whom records these varieties of information are kept has included an appropriate notice requirement delineating observation, collection, retention and use policies and a explicit and clear consent provision, then the requirements of Article 2b may effectively have been met. *See* Section III.C(3) below.

66. *See, e.g.*, N.H. REV. STAT. ANN. § 644:9 (2024).

C. "natural, essential, and inherent."

The Article 2b analysis does not end with the application of the definition of "personal or private information." The analysis must also consider whether the intrusion survives a strict scrutiny analysis in light the right to be free of intrusion on the defined information is "natural, essential, and inherent."

1. Analytical Framework

The language of Article 2b creates a fundamental right, thus the description of the right as natural, essential, and inherent. The "natural, essential, and inherent" language is taken directly from Part I, Article 2 itself.[67] It is the first and the most foundational description of protected rights in the New Hampshire Constitution.

Unlike Art. 19, it does not use a modifier to condition the right, like "unreasonable." It also does not mention search warrants supported by probable cause. It creates an unconditioned and unambiguous fundamental right. Consequently, courts should view any intrusion on personal or private information as directly affecting a fundamental right in freedom from intrusion on that information. Any such intrusion deprives one of that fundamental right.

It is not the case that any governmental intrusion on personal information is absolutely prohibited in every circumstance. Instead, Article 2b should invoke a strict scrutiny analysis. "To comply with strict judicial scrutiny, the governmental restriction must 'be justified by a compelling governmental interest and must be necessary to the accomplishment of its legitimate purpose.'"[68]

The written testimony of one of the authors before the Senate Rules and Enrolled Bills Committee captures this intention:

> CACR 16 does not prohibit any and all access to personal and private information. Those who say so are either misunderstanding its legal effect or greatly exaggerating its effect.
>
> Instead, it would effectively change the balancing a court already does when deciding whether the

67. "All men have certain natural, essential, and inherent rights among which are, the enjoying and defending life and liberty; acquiring, possessing, and protecting, property; and, in a word, of seeking and obtaining happiness. Equality of rights under the law shall not be denied or abridged by this state on account of race, creed, color, sex or national origin." Article 2b.

68. Akins v. Sec'y of State, 904 A.2d 702, 707–08 (N.H. 2006) (quoting Follansbee v. Plymouth Dist. Ct., 856 A.2d 740, 743 (N.H. 2004)).

> governmental interest in gaining such access outweighs the nature and degree of intrusion on an individual's privacy interest. Specifically, it would require the government to now show a compelling state interest in obtaining access to personal and private information before a court would order such access. Sometimes, the state will be able to meet that burden, particularly when public safety is at risk.[69]

It may well be that the government has a compelling interest in gathering certain kinds of personal information. If so, the particular kind of intrusion must be *necessary* to accomplish that purpose. It is not sufficient that the intrusion is one way to accomplish the purpose but that other ways also exist. Bluntly, it must be the only way. For example, if another way exists but it is more cumbersome or expensive, then the intrusion on the compelling interest is not enough, that is, it is not necessary. Nor is the justification that it would be useful to have the personal information enough to merit identification as a *compelling* interest. Any intrusion on the direct fundamental right is constitutionally significant enough and so requires a *compelling* governmental interest implemented in a way that is *necessary*, not merely convenient or most practical.

At first blush, this burden may seem onerous and prone to invalidate any number of well-established government efforts to collect personal information. It may well be that the government has been what will now be viewed as over-reaching in some of its efforts to collect personal information. Article 2b means that society, via the courts, must take a fresh look at the extent to which government collects personal information. Again, an individual's control of their personal information is constitutionally prioritized over the interests of the government.

2. Intersection with Part I, Article 19

Article 19 is also a privacy amendment. As noted above, it indirectly protects personal information in certain locations and containers, using a reasonable-expectation-of-privacy analysis. This requires: "first, that a person have exhibited an actual (subjective) expectation

69. *Constitutional Amendment Concurrent Resolution 16: Hearing on 2018-1936e Before the Senate Rules and Enrolled Bills Committee*, 2018 (N.H. 2018) (written testimony of Albert (Buzz) Scherr).

of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable."[70]

With Article 2b now adopted, it has the effect of constitutionalizing "personal information" as something in which an individual has a reasonable expectation of privacy. That is, by virtue of the popular support for Article 2b,[71] society has said both that one has an expectation of privacy in personal information and that society views that expectation as reasonable.

For example, in 2011 (seven years before Article 2b was enacted), the New Hampshire Supreme Court concluded that one does not have a reasonable expectation of privacy in one's internet service subscriber information. Thus, the government's collection of that information does not count as a search under Article 19 and a warrant (or an exception) is not necessary.[72] With Article 2b now in the Constitution, not only a new, Article 2b analytical framework is in effect concerning the internet service subscriber information; but also the question *under Article 19* now becomes whether internet service subscriber information is "personal information." If it is, then the reasonable-expectation-of-privacy requirement has been met. Note that this does not end that kind of police investigation, it simply requires that the government obtain a search warrant supported by probable cause or meet an established warrant exception. And, this analysis occurs separately from any Article 2b strict scrutiny analysis.

In addition, the adoption of an Article 2b analytical framework must not involve the adaptation of Art. 19's analytical framework. Article 2b and Art. 19 are very differently worded. Article 2b contains no reference to a search warrant supported by probable cause. The reasonable-expectation-of-privacy standard was not intended to be a part of any Article 2b analysis. One drafter and the prime sponsor of Article 2b has said:

> So why do we need this amendment? The U.S. Supreme Court has established a two-part test to determine whether personal information can be seized by the government. First, the individual must demonstrate an expectation of privacy, i.e. do something, like closing a door, to show that privacy is desired, and second the expectation of privacy must be reasonable.

70. State v. Goss, 834 A.2d 316, 319 (N.H. 2003).
71. Over 81% voted in favor of the amendment.
72. *See* State v. Mello, 27 A.3d 771, 774–75 (N.H. 2011).

> Unfortunately, courts and ordinary people don't think the same things are reasonable. Most people would think that they haven't surrendered their DNA by dining out and they haven't made their personal thoughts public by sending texts and emails. Courts think those things are not private. Texts and emails are not encrypted, so anyone with the right equipment can read them. Similarly, you didn't take that fork to the bathroom and wash it.
>
> We need this amendment so that, at least in New Hampshire, *ordinary peoples' expectation of information privacy is the norm*, not the exception, and government "snooping" into our personal and private information is prohibited.[73]

The analytical framework for Article 2b must start with a clean slate. Otherwise, the adoption of an Article 19 framework renders Article 2b a mere sub-set of Article 19, a result specifically not intended as shown by its separate and primary placement in the constitution

3. Consent

Practically, Article 2b's power is not absolute. The government has the ability to build consent provisions into personal-information collection. If the government were to include opt-in provisions in personal-information-gathering statutes, it will have effectively obtained consent for the collection of that information. Done correctly under Article 2b, an opt-in provision would need to provide explicit notice of what the government specifically intended by the observation, collection, retention and use of the information. The subsequent observation, collection, retention, and/or use must also not exceed that to which consent was given.

The New Hampshire legislature has shown the capability of making this adaptation to governmental information-collecting processes. In the 2021–2022 legislative session, it amended RSA 141-C:20-f to add the following new paragraph:

> II-a. Each patient, or the patient's parent or guardian if the patient is a minor, shall be given the opportunity to opt-out or opt-in to the immunization registry. No patient's personal data, such as name, address, date of birth, immunization, or vaccination information, shall

73. Neal Kurk, *Vote for Your Privacy on Question 2*, UNION LEADER (Nov. 2, 2018), https://perma.cc/A2EJ-UT5U.

> be entered into the registry without the explicit, written or electronic consent of the patient, or the patient's parent or guardian.[74]

In the 2020–2021 session, the legislature added an explicit consent requirement to consensual car searches. It required that a police officer who has requested to search an individual's car both inform the driver that they have a constitutional right to refuse to consent and obtain documentation of the driver's consent to have the car searched. Without such proof, the results of a consensual search would be inadmissible.[75] Prior to passage of this provision, an officer did not have to either inform the driver of this constitutional right or document any such consent. Though the driver already had that constitutional right, the legislature saw fit to amend the statute to embed a much more explicit set of consent requirements, effectively a documented opt-in provision.

Thus, the legislature has shown that it is capable of making whatever adaptations are necessary to meet the kind of constitutional requirement imposed by Article 2b. Going forward, Article 2b effectively *requires* constitutionally sufficient respect for an intrusion on personal or private information. To paraphrase then Representative Kurk's statement: the state must respect that *ordinary peoples' expectation of information privacy is now the norm, not the* exception.[76]

CONCLUSION

21st century information is not 18th century information. The types and nature of information and the ways to access information are ever-expanding. They are profoundly different from that which existed or was even contemplated in the 18th century when Part I, Article 19 of the New Hampshire Constitution was written. Individuals are losing ground in their ability to keep control of their personal information as Article 19 and the Fourth Amendment remain too frequently bound in by the limits of the location/container paradigm even amidst the reasonable-expectation-of-privacy analysis. And even today, we cannot even conceive of the forms and types of access to information that the future holds.

---

74. N.H. REV. STAT. ANN. § 141-C:20-f (passed June 24, 2022; effective date July 1, 2023.)

75. N.H. REV. STAT. ANN. § 595-A:10 (2021).

76. GDPR, art. 4(1).

Article 2b is a statement of principle about information privacy for the present and the future. It updates New Hampshire citizens' right to be "left alone;" to be the ones in control of their personal information in the first instance, not the state. Different people draw different lines when it comes to which of their information should be private. Therein lies much of the essence of privacy—it is intensely personal. Part I, Article 2b gives the individual, in the first instance, the right to draw those lines, not the government. It exists as a forward-looking principle designed for the individual.

More broadly, Article 2b operates as a 21st century "ordinance of the people" and "a dynamic set of substantive instructions and limitations on government that is adopted and jealously maintained by the people themselves."[77] The constitutional amendment process in New Hampshire is a difficult one. Yet, Article 2b reflects a strong popular will to rein in government conduct regarding personal and private information. Rather than an experiment in the laboratory of state constitutional jurisprudence, Article 2b stands as a model statement of principle sensitive to both current and a forward-looking perspective.

77. Marshfield, *supra* note 3, at 859–60.