NORTH CAROLINA LAW REVIEW

Volume 94 | Number 3 Article 7

3-1-2016

Biometric Data Collection and RFID Tracking in Schools: A Reasoned Approach to Reasonable Expectations of Privacy

Stefan P. Schropp

Biometric Data Collection and RFID Tracking in Schools: A Reasoned Approach to Reasonable Expectations of Privacy*

> *That they are educating the young for citizenship is reason for scrupulous protection of Constitutional freedoms of the individual, if we are not to strangle the free mind at its source and teach youth to discount important principles of our government as mere platitudes.*[1]

INTRODUCTION

At a time when many have decried the seemingly glacial pace at which this nation's public schools have incorporated technology into their pedagogical practices,[2] twenty-first century advances are revolutionizing other aspects of the educational experience. Among these changes, the collection and use of biometric information—uniquely identifiable physical characteristics ranging from fingerprints, to palm prints, to iris or retina patterns[3]—have been implemented in more than one thousand school districts in forty states,[4] with some of these schools also tracking students' movements

1. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 637 (1943).

2. *See, e.g.*, Darrell M. West & Joshua Bleiberg, *Five Ways Teachers Can Use Technology to Help Students*, BROOKINGS (May 7, 2013), http://www.brookings.edu/research/opinions/2013/05/07-teachers-technology-students-education-west-bleiberg [http://perma.cc/3DBH-N8AX] ("Technology has failed to transform our schools . . . ."); Ryan Lytle, *Teacher Training Needed to Meet Technology Needs in Classrooms*, U.S. NEWS & WORLD REP. (Sept. 20, 2012, 10:30 AM), http://www.usnews.com/education/high-schools/articles/2012/09/20/teacher-training-needed-to-meet-technology-needs-in-classrooms [http://perma.cc/7CVM-BEZ4] (detailing a survey of "high school and college students, teachers, and parents in the United States, China, and Germany" finding that "82 percent [of respondents] across the globe also noted that technology needs to play a bigger role in classrooms"); Linda Starr, *Encouraging Teacher Technology Use*, EDUC. WORLD, http://www.educationworld.com/a_tech/tech159.shtml (last updated Mar. 31, 2012) [http://perma.cc/VNP8-6WPR] ("Some teachers, experts say, still are reluctant to use technology, mostly because of a lack of time, a lack of resources, or a lack of confidence in their ability to use the available technology.").

3. *See infra* Section I.A.

4. Jeffrey Stinson, *As Florida Bans Use of Biometric IDs in Schools, Other States Scale Back on Big Brother*, FLAGLERLIVE.COM (Nov. 2, 2014), http://flaglerlive.com/72393/children-biometrics/ [http://perma.cc/Y53H-4K7A] ("Jay Fry, CEO of the biometric-in-schools firm identiMetrics, said biometric identification is used in more than 1,000 school districts in 40 states from Alaska to Long Island, New York. West Virginia uses the technology in 70 percent of its 57 school districts . . . ."). *But see id.* ("Several states are

through microchips.[5] The new technology promises increased efficiency and improved student outcomes on a range of daily activities in the life of a student with applications from the lunch line to the library and the school bus to the classroom.[6]

But despite the technologies' promise, these advances have not come without their fair share of detractors. A nascent body of scholarly work,[7] a passionate and growing cluster of advocacy groups,[8] and a patchwork of legislative proposals[9] have critically reviewed the security concerns and potential for malfeasance inherent in biometric data collection and radio-frequency identification ("RFID") tracking. These critiques have ranged from the purely rhetorical[10] to the perfectly well reasoned[11] and have come from both ends of the traditional political spectrum.[12]

now banning or restricting the use of the technology in schools, as worries over student privacy have risen amid breaches of government and commercial computer databases.").

5. *See infra* Section I.A.

6. *See infra* Section III.C.

7. *See, e.g.*, Nicole A. Ozer, *Rights "Chipped" Away: RFID and Identification Documents*, 2008 STAN. TECH. L. REV. 1, ¶¶ 26–43 (2008) (section entitled "Insecure RFID Technology Interferes with Constitutional Rights"); Alexandra C. Hirsch, Comment, *Schools: Where Fewer Rights Are Reasonable? Why the Reasonableness Standard Is Inappropriate to Measure the Use of RFID Tracking Devices on Students*, 28 J. MARSHALL J. COMPUTER & INFO. L. 411, 411–14 (2011).

8. *See, e.g.*, AGAINST RFID IN SCHOOLS, http://rfidinschools.com (last updated Mar. 17, 2015) [http://perma.cc/8CC7-MUU6]; Paul Joseph Watson, *Texas Students Revolt Against Mandatory RFID Tracking Chips*, INFOWARS (Aug. 30, 2012), http://www.infowars.com/texas-students-revolt-against-mandatory-rfid-tracking-chips/ [http://perma.cc/J2KK-HVD4].

9. *See infra* Section IV.A.

10. Take, for example, the comments of Missouri State Senator Ed Emery who sponsored the legislation prohibiting the use of RFID tracking in schools and believes "[t]here's a 'Big Brother' quality to this." Jeffrey Stinson, *States Backtrack on Student Tracking Technology*, STATELINE (Oct. 27, 2014), http://www.pewtrusts.org/en/Research-and-Analysis/Blogs/Stateline/2014/10/27/States-Backtrack-on-Student-Tracking-Technology [http://perma.cc/98ZA-VVHT].

11. *See, e.g.*, *id.* ("[L]awmakers [should] focus on transparency so parents know how the technology is being used, what data is collected and what safeguards are in place to protect students' privacy.").

12. Opposition to this technology has come from Republicans like Missouri State Senator Ed Emery and Florida State Senator Dorothy Hukill, who both sponsored legislation limiting or prohibiting its use. *See id;* Act of May 12, 2014, ch. 2014-41, § 2, 2014 Fla. Laws 798, 799 (codified at FLA. STAT. § 1002.222 (West, Westlaw through 2015 Spec. A Sess.)); Act of Sept. 10, 2014, 2014 Mo. Legis. Serv. 137, 137 (West) (codified at MO. REV. STAT. § 167.168 (West, Westlaw through 2014 Mo. Gen. Assemb. 2d Reg. Sess.)). It has also come from Democrats like former Rhode Island State Senator John Tassoni, who sponsored the legislation in his state to ban the use of RFID tracking in schools. *See* S.B. 211, 2009 Gen. Assemb., Jan. Sess. (R.I. 2009); Claire Swedberg, *Rhode Island Governor Vetoes Restrictions on RFID*, RFID J. (Nov. 12, 2009), http://www.rfidjournal.com/articles/view?5377 [http://perma.cc/7D7K-WDZ7].

Given the developing nature of literature in this field to date, it is important to note at the outset exactly where this Recent Development fits—what it is and, more importantly, what it is not. It is not an Orwellian "parade of horribles," imagining a world where "every sound you made was overheard, and, except in darkness, every movement scrutinized."[13] Nor is it an attempt to account for the more well-founded fears that, in a world where even the wealthiest multinational corporations are subject to data breaches,[14] perhaps even well-intentioned (but admittedly underfunded) school districts are not the appropriate repositories for sensitive personal information. Each of these approaches grapples with the compelling concerns that are raised when this technology is not used as it was intended—when something goes wrong.

This Recent Development seeks to address the different but equally important concern that is raised when this technology works *exactly* as it was intended—when it goes according to plan. In its intended and most benign form, this technology necessarily requires trade-offs between students' privacy and school efficiency and security that threaten wolf-like encroachments on the Fourth Amendment cloaked in the sheep's clothing of twenty-first century advancement. Accordingly, this Recent Development seeks to test the constitutional support for the widespread collection of public school students' unique biometric information. Moreover, it provides a framework for state legislatures to evaluate these trade-offs and decide for themselves—and for their students—whether the gains are worth the cost. This Recent Development freely admits, as did the Supreme Court over a century ago, that such compromises "may be . . . the obnoxious thing in its mildest and least repulsive form"[15]

13. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 5 (1949).

14. *See, e.g.*, Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, N.Y. TIMES (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0 [http://perma.cc/JTM5-L9AK (dark archive)]; Jordan Robertson, *Which Big Retailer Hasn't Reported a Major Breach—Yet?*, BLOOMBERG BUS. (Oct. 21, 2014, 7:02 PM), http://www.bloomberg.com/news/articles/2014-10-21/which-big-retailer-hasn-t-reported-a-major-breach-yet- [http://perma.cc/C64D-U8FW].

15. Boyd v. United States, 116 U.S. 616, 635 (1886). Indeed, the Court has often rebuked the slow erosion of privacy rights. *See generally id.* ("It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon. Their motto should be *obsta principiis*."); Osborn v. United States, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting) ("These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society

but ultimately concludes, as that Court acknowledged, that to do nothing risks the greater harm of allowing "illegitimate and unconstitutional practices [to] get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure."[16]

Analysis proceeds in four parts. Part I provides an overview of the field of biometrics and RFID technology with emphasis on school-specific applications of the technology. Part II examines the Fourth Amendment issues raised by the proliferation of this technology in schools and details the case law that provides a foundation for analysis. Part III analyzes the competing interests under consideration in this context using the Supreme Court's Fourth Amendment framework and attempts to balance the needs of the school with the interests of the student. Finally, Part IV details the legislative responses to this point and suggests a comprehensive plan to ameliorate the concerns while preserving the benefits of these programs.

I. BIOMETRICS

Biometrics refers to the measurement of an individual's unique physical characteristics and the matching of those characteristics against previously recorded information to determine a person's identity.[17] Biometric data collection "is the process whereby biometric measurements are collected and integrated into a computer system, which can then be used to automatically recognize a person."[18] Biometric data collection and scanning can serve two different purposes.[19] The first, known as identification, compares biometric information against all previously stored information and makes a "one-compared-to-many match."[20] In the education context, this function allows a computer to uniquely identify a student from a database containing data on every student in a population. The

quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.").

16. *Boyd*, 116 U.S. at 635.

17. *See* Anil Jain, Lin Hong & Sharath Pankanti, *Biometric Identification*, 43 COMM. ACM 91, 92 (2000); Rajiv Chandrasekaran, *Brave New Whorl*, WASH. POST (Mar. 30, 1997), https://www.washingtonpost.com/archive/business/1997/03/30/brave-new-whorl/6e618930-9765-43a3-803c-94a589d266d0/ [https://perma.cc/D9CX-XPL9].

18. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 100 (1997).

19. *See id.*

20. *See id.*; *see also* Rudy Ng, Note, *Catching Up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology*, 28 HASTINGS COMM. & ENT. L.J. 425, 428 (2006).

second, known as verification, compares the biometric information only to the stored information for the claimed identity and searches for a "one-to-one" match.[21] A verification system can only confirm that students are who they claim to be but does not allow the system to identify a particular student against all students in a population. In addition to public schools, both private[22] and other public-sector entities[23] have begun widespread use of biometric collections and scanning.[24]

While the types of biometric information available to law and immigration enforcement have expanded rapidly in recent years—and may one day present an issue for public schools—the collection of biometric information from students is more limited. Accordingly, this Recent Development is limited to the three primary biometric and tracking technologies currently available to schools: (1) fingerprint or palm scans; (2) iris scans; and (3) the use of RFID tracking. These methods of collection and their applications are discussed below.

A. Fingerprint and Palm Scans

Law enforcement has used fingerprints for identification since the early twentieth century, making fingerprints "the most common and widely accepted form of biometric identification."[25] However, in a recent push toward increased efficiency and security, schools across the country have turned to fingerprint scanners in both their lunch

21. *See* Woodward, *supra* note 18, at 100; *see also* Ng, *supra* note 20, at 428.

22. Although not the focus of this Recent Development, private organizations—from Disney theme parks to banks and credit card companies to private gyms—now use customers' biometric identification. *See* Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1532 (2013).

23. While this Recent Development focuses specifically on the use of biometrics in public K–12 education, other examples of government use of biometrics include the Secure Communities program (requiring biometric database screening of anyone apprehended by state and local law enforcement), United States Visitor and Immigrant Status Indicator Technology (requiring fingerprint collection of all non-citizen visitors to the United States), and U.S. Passports and e-Passports programs (requiring a digital photo that is provided to a centralized facial recognition database). *See id* at 1531–33.

24. *See, e.g.*, Woodward, *supra* note 18, at 97–98, 98 n.6.

25. Ng, *supra* note 20, at 429; *see also* John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 70 (2002) ("While fingerprinting is probably the most common and widely known form of biometric identification, it is by no means the only example."); Woodward, *supra* note 18, at 104.

lines[26] and their libraries.[27] Unlike traditional law enforcement techniques, which compare the unique ridge formations of the entire fingerprint,[28] most school-based systems scan only a portion of a student's fingerprint.[29] According to the companies producing and promoting the technology, this reduces or eliminates the potential for duplication and identity theft.[30] Similarly, many school districts have implemented palm scanners, which, rather than scanning the entire palm, evaluate "the unique squiggle of lines made by the veins inside the hand" and "convert[] the scanned veins to a numeric value that matches each student in a database."[31] While these systems prevent the duplication of fingerprint and palm scans and thereby reduce the risk of identity theft, they must also be able to match biometric information to an individual student using the one-to-many identification approach of biometrics.

B. Iris Scans

A second area of growth in biometric data collection of K–12 students is the expanded use of iris scans—particularly on school buses.[32] The iris is the colored portion of the eye, surrounding the pupil, that contains a number of structures that can be used to uniquely identify an individual.[33] An image of the iris is captured using a high-resolution camera and then compared to previously recorded and stored images.[34] Several companies[35] have developed

26. *See, e.g.*, *School Cafeterias Trading Lunch Money for Fingerprint Scans*, CBS CHI. (July 2, 2014, 12:49 PM), http://chicago.cbslocal.com/2014/07/02/school-cafeterias-trading-lunch-money-for-fingerprint-scans/ [http://perma.cc/4VYV-VT4W].

27. *See, e.g.*, *Best Practices—Technology: This Minnesota High School Gives Fingerprint Scanning a Whorl*, ESCHOOL NEWS (Sept. 1, 2000), http://www.eschoolnews.com/2000/09/01/b-best-practices-b-technology-this-minnesota-high-school-gives-fingerprint-scanning-a-whorl/ [http://perma.cc/SE33-JRP8].

28. *See, e.g.*, Ng, *supra* note 20, at 429.

29. *School Cafeterias Trading Lunch Money for Fingerprint Scans*, *supra* note 26.

30. *Id.*; *see also The identiMetrics Finger Scanning ID System*, IDENTIMETRICS, http://www.identimetrics.net/index.php/products/the-identimetric-finger-scanning-id-system [https://perma.cc/E8MF-VTNY] ("Fingerprints cannot be recreated from the encrypted numerical templates. Student accounts cannot be compromised.").

31. James L. Rosica, *Biometrics May Be Banned in Florida Schools, but Flourish Elsewhere*, TAMPA TRIB. (Mar. 9, 2014), http://tbo.com/news/politics/biometrics-may-be-banned-in-florida-schools-but-flourish-elsewhere-20140309/ [http://perma.cc/354L-S2WC].

32. *See* Laurie Segall & Erica Fink, *Iris Scans Are the New School IDs*, CNN MONEY (July 11, 2013, 10:42 AM), http://money.cnn.com/2013/07/11/technology/security/iris-scanning-school/ [https://perma.cc/K73G-67BL].

33. Ng, *supra* note 20, at 431.

34. *Id.*

35. *See, e.g.*, BLINKSPOT, http://www.blinkspot.com [http://perma.cc/Z9MY-45Y8]; EYELOCK, http://eyelock.com/index.php/products/nano-nxt [http://perma.cc/GJ2M-ZYHP].

iris scanners specifically for use on school buses.[36] The technology allows a student to look into a scanner (resembling a pair of binoculars) and have his identity matched to those iris scans already in the system.[37] Once the system finds a match, it notifies the student and the driver that the student is on the correct bus and allows parents and school administrators to track the location of the student.[38] As with fingerprint and palm scans, advocates of the system note that the data is encrypted and converted to a numeric code to prevent identity theft.[39] However, like all school-based biometric information, iris scans use a one-to-many matching system that would allow schools, which own the biometric data,[40] to match an available iris image to the existing database.

C. Radio Frequency Identification

While it is not a biometric measurement in the traditional sense, the advent and expanded use of RFID tracking shares the unique identification and one-to-many matching capabilities of fingerprints and iris scans. Since RFID technology originally appeared during World War II, "significant improvements in functionality; decreases in both size and costs, especially in the last decade; and agreements on communication standards have combined to make the technology [newly] viable" for a variety of purposes.[41]

RFID systems consist of three components: a microchip, a reader, and a database.[42] In a school-based RFID system, schools may require students to carry the microchip (typically embedded in an ID badge or sewn into a backpack) with them at all times.[43] The chip can communicate with readers in one of two ways.[44] First, in a passive system, the microchip communicates with the reader only when

36. Segall & Fink, *supra* note 32 (explaining how Blinkspot and Eyelock's technology can be used to track children when they board school buses).

37. *See id.*

38. *Id.*

39. *Id. But see* David Goldman, *Hackers' Next Target: Your Eyeballs*, CNN MONEY (July 26, 2012, 12:24 PM), http://money.cnn.com/2012/07/26/technology/iris-hacking/index.htm?iid=EL [http://perma.cc/WMU8-CRB4] (noting that the susceptibility of fingerprint and iris scans to reverse-engineering poses a huge problem).

40. *See* Segall & Fink, *supra* note 32 (noting that "the companies themselves don't collect any of the data—the schools . . . that use them own the data").

41. DAVID C. WYLD, RFID: THE RIGHT FREQUENCY FOR GOVERNMENT 5 (2005), http://www.businessofgovernment.org/sites/default/files/RFIDReport.pdf [http://perma.cc/ZE8F-AKNW].

42. Margaret L. Lorenc, Comment, *The Mark of the Beast: U.S. Government Use of RFID in Government-Issued Documents*, 17 ALB. L.J. SCI. & TECH. 583, 586 (2007).

43. *See* Hirsch, *supra* note 7, at 419.

44. *Id.* at 416.

prompted—such as when placing a card with an embedded microchip near a locked door or when passing by a reader placed in the hallway.[45] Conversely, in an active system, the microchip is in constant communication with the reader and provides consistent and real-time information on the location of the student.[46] Finally, in both versions a central database serves as a storage location for information that allows authorized computers to access information stored in the system.[47] This information includes not only the location and movements of the RFID chip but also any stored information unique to the chip's owner—including name, photo, and other biometric indicators (such as fingerprint, palm print, or iris scan information).[48]

While both supporters and opponents of RFID use in schools continue to debate the security these systems provide from identity theft,[49] the importance of these systems to this Recent Development is that they serve both functions of a biometric scanner: the one-to-one verification—confirming that a student was where she claims to have been—and the one-to-many identification—determining which student was in a particular location at a given time. Notwithstanding the security and privacy concerns,[50] several school districts—in states from Texas[51] to New Jersey[52] to California[53]—have moved forward

45. *Id.* at 415–16.

46. *Id.*

47. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-551, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 1, 4, 9 (2005).

48. *See id.* at 9 (noting that the "type of information housed in the database will vary by application" but can include "item identifier, description, manufacturer, movement of the item, and location").

49. *Compare* Hirsch, *supra* note 7, at 411–12 (suggesting that to steal RFID information "all a determined delinquent must do is identify a target school experimenting with the new safety system, pull a car up outside the building, and wait"), *with* Jennifer Radcliffe, *Tracking Devices in School Badges Raise Concerns*, HOUS. CHRON. (Oct. 11, 2010, 5:30 AM), http://www.chron.com/neighborhood/spring-news/article/Tracking-devices-in-school-badges-raise-concerns-1716571.php [http://perma.cc/Y6RN-QMFS] ("It's a very secure system [with] no data to confirm that there's any . . . safety risks.").

50. While the concern with data security and identity theft has been covered in this Section, the remainder of the Recent Development focuses exclusively on the Fourth Amendment privacy concerns raised by these systems.

51. *See* Radcliffe, *supra* note 49 (detailing the implementation of RFID tracking in two Houston-area school districts).

52. *See* Claire Swedberg, *New Jersey Schools Adopt RFID to Secure Their Facilities*, RFID J. (Sept. 6, 2013), http://www.rfidjournal.com/articles/view?10971/ [http://perma.cc/N2FJ-BNZB] (describing the implementation of RFID tracking systems in all of a New Jersey district's schools and in twenty-one of the district's buses).

53. *See* Letter from Nicole A. Ozer, Tech. & Civil Liberties Policy Dir., ACLU of N. Cal. & Lee Tien, Sr. Staff Att'y, Elec. Frontier Found., to Daniel R. Levinson, Inspector Gen., U.S. Dep't of Health & Human Servs. & Joe Valentine, Dir., Emp't & Human

with the implementation of RFID tracking programs in their schools. While these security concerns deserve the continued discussion they are receiving, the next Part instead focuses on the constitutional issues raised by the implementation of these systems.

II. FOURTH AMENDMENT PROTECTIONS IN THE SCHOOL CONTEXT

Children, like adults, enjoy the protections afforded by the Fourth Amendment—incorporated against the states through the Fourteenth Amendment—from unreasonable governmental searches and seizures.[54] However, unlike adults, those protections are modified in the school setting to reflect the responsibility of the school to safeguard and educate the nation's youth.[55] This Part looks briefly at the historical context of the Fourth Amendment before detailing the Supreme Court's framework for analyzing its protections inside the schoolhouse doors.

A. The Fourth Amendment Standard

The Fourth Amendment to the Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[56] As the Supreme Court has noted, "[t]he . . . historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects."[57] Indeed, even among the sacred protections enshrined in the Bill of Rights, those afforded by the Fourth Amendment are arguably the most zealously guarded by the Court.[58]

Servs. Dep't (Sept. 14, 2010), https://www.aclunc.org/sites/default/files/asset_upload_file994_9490.pdf [http://perma.cc/3L48-L6LS] (detailing attempts to implement RFID tracking in California schools).

54. *See infra* notes 60–63 and accompanying text.

55. *See infra* notes 63–67 and accompanying text.

56. U.S. CONST. amend. IV.

57. Olmstead v. United States, 277 U.S. 438, 463 (1928).

58. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968) (quoting Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891)) ("No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."); *see also* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 564 (1990) (noting that the "fourth amendment protection [is] the single most important characteristic which distinguishes a free society from a police state"). *But see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004) ("When technology is new or in flux, and its use may have privacy implications far removed from property law, Fourth Amendment rules alone will tend not to provide adequate privacy protections.").

Moreover, while the historical underpinnings of the Fourth Amendment point to a desire to prevent the reappearance of "the pre-Revolutionary practice of using general warrants or 'writs of assistance' to authorize searches for contraband by officers of the Crown," the Court has expanded its protections beyond those police actions and has instead imposed its restrictions on all governmental action.[59]

B. The Fourth Amendment Goes to School

For the better part of the last century, the notion that the Fourth Amendment, as incorporated against the states through the Fourteenth Amendment,[60] "protects the rights of students against encroachment by public school officials" has been, in the Supreme Court's estimation, "indisputable."[61] Indeed, at one point it seemed as though the Court was willing to match the constitutional rights of children within the schoolhouse to those of citizens outside it:

> The Fourteenth Amendment, as now applied to the States, protects the citizen against the State itself and all of its creatures—Boards of Education not excepted. These have, of course, important, delicate, and highly discretionary functions, *but none that they may not perform within the limits of the Bill of Rights*.[62]

However, since that time, the Supreme Court has slowly eroded the Fourth Amendment protections afforded to students who cross the schoolhouse threshold. Despite repeated assurances that students do not "shed their constitutional rights . . . at the schoolhouse gate,"[63] the Court's subsequent refinement has left students with Fourth Amendment rights that "are different in public schools than elsewhere" given that "the 'reasonableness' inquiry cannot disregard the schools' custodial and tutelary responsibility for children."[64] The

59. New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) (quoting Burdeau v. McDowell, 256 U.S. 465, 475 (1921)) (describing the Fourth Amendment's restrictions as "upon the activities of sovereign authority").

60. U.S. CONST. amend. XIV.

61. *T.L.O.*, 469 U.S. at 334.

62. *Id.* (emphasis added) (quoting W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 637 (1943)).

63. Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503, 506 (1969). Although *Tinker* considered First Amendment issues in the school context, the Court has adopted similar language in the context of school searches and seizures as well. *See, e.g.*, *T.L.O.*, 469 U.S. at 334 ("Equally indisputable is the proposition that the Fourteenth Amendment protects the rights of students against encroachment by public school officials . . . .").

64. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 656 (1995).

Court has likewise found the probable cause standard of reasonableness, as applied in the criminal context, to "be unsuited to determining the reasonableness of administrative searches where the [g]overnment seeks to *prevent* the development of hazardous conditions"[65] and "unnecessary in the public school context because such requirements 'would unduly interfere with the maintenance of the swift and informal disciplinary procedures that are needed.' "[66] Therefore, it seems clear that the side of the Fourth Amendment's balancing test weighted by the student's legitimate expectation of privacy "is limited in a public school environment where the State is responsible for maintaining discipline, health, and safety."[67]

In the context of school searches, to determine the constitutional reasonableness of a search the courts must "engage in a fact-specific 'balancing' inquiry, under which the magnitude of the government's need to conduct the search at issue is weighed against the nature of the invasion that the search entails."[68] Under this test, "[o]n one side of the balance are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order."[69] To aid in this fact-specific inquiry, the Supreme Court has developed a framework that instructs a reviewing court to "consider first the 'scope of the legitimate expectation of privacy at issue,' then the 'character of the intrusion that is complained of,' and finally the 'nature and immediacy of the governmental concern at issue' and the efficacy of the means employed for dealing with it."[70]

Unfortunately, the Supreme Court's jurisprudence on Fourth Amendment protections in schools—even applying the three-part framework described above—does precious little to illuminate the constitutional boundaries of biometric data collection and RFID tracking. In the Court's two leading cases, plaintiffs challenged the random drug testing of student athletes and others participating in extracurricular activities.[71] In both of those cases, the Court relied

65. Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls, 536 U.S. 822, 828 (2002) (quoting Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989)).

66. *Id.* at 828–29 (quoting *Acton*, 515 U.S. at 653).

67. *Id.* at 830.

68. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 352 (8th Cir. 2004) (quoting *T.L.O.*, 469 U.S. at 337).

69. *Id.* (quoting New Jersey v. T.L.O., 469 U.S. 325, 337 (1985)).

70. *Id.* at 352 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–66 (1995)).

71. *Earls*, 536 U.S. at 822 (challenging a policy that "requires all middle and high school students to consent to urinalysis testing for drugs in order to participate in any

heavily on the fact that the activities in question were voluntary to find that the students had a reduced expectation of privacy[72]—a conclusion that does little to help gauge a student's privacy interest where, as in the case of biometric tracking, the activity is compulsory.[73] Similarly, in *New Jersey v. T.L.O.*,[74] the Court considered whether an administrator could reasonably search a student's bag upon suspicion that the student had been smoking cigarettes in the bathroom[75]—an analysis which sheds little light on systematic or ongoing searches and surveillance. A recent Supreme Court decision holding that the strip-search of a thirteen-year-old girl was too intrusive to be constitutionally permissible—even with reasonable suspicion—similarly provides very little guidance upon which to begin an analysis.[76]

However, a growing body of lower-court jurisprudence provides the sketches of a boundary line to demarcate the legitimate interests of the student and the needs of the school as they relate to ongoing searches. For example, the Eighth Circuit recently held that random, suspicionless searches of a student's person and possessions ran far afoul of constitutionally permitted activity.[77] Despite noting that students have a lower expectation of privacy inside the schoolhouse, the court held that a "search of a child's person . . . is undoubtedly a severe violation of subjective expectations of privacy."[78] While noting the generalized concerns expressed by the school district regarding the presence of weapons and drugs in its schools, the court poignantly noted that "[a]ll schools surely have an interest in minimizing the harm that the existence of weapons and controlled substances might visit upon a student population, but public schools have never been entitled to conduct random, full-scale searches . . . because of a mere

extracurricular activity"); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 648 (1995) (challenging a program that "authorizes random urinalysis drug testing of students who participate in . . . school athletics programs").

72. *See Earls*, 536 U.S. at 823 ("In any event, students who participate in competitive extracurricular activities voluntarily subject themselves to many of the same intrusions on their privacy as do athletes."); *Acton*, 515 U.S. at 657 ("By choosing to 'go out for the team,' they voluntarily subject themselves to a degree of regulation even higher than that imposed on students generally.").

73. *See infra* notes 112–115 and accompanying text.

74. 469 U.S. 325 (1985).

75. *Id.* at 347 (finding the "search resulting in the discovery of the evidence of marihuana dealing" to be reasonable).

76. Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 379 (2009).

77. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 354 (8th Cir. 2004).

78. *Id.*

apprehension."[79] Therefore, at least in the absence of particularized suspicion, the court was willing to find that ongoing and systematic searches were an unconstitutional invasion of privacy.

Similarly, the Ninth Circuit has held that random and suspicionless use of drug-sniffing dogs (something at least one other circuit has offered as an effective and minimally intrusive measure)[80] violates the Fourth Amendment.[81] Despite noting the important—potentially even compelling—government interest at stake, the court concluded that "[i]n the absence of a drug problem or crisis . . . the government's important interest in deterring student drug use would not have been 'placed in jeopardy by a requirement of individualized suspicion.' "[82] Importantly, despite another court holding that the use of dogs was minimally intrusive[83]—an argument that could be advanced by proponents of RFID tracking, fingerprinting, and iris scanning—the Ninth Circuit still required individualized suspicion prior to the search.

C. The Intersection of Biometric Data and the Fourth Amendment

Before balancing the students' reasonable expectations of privacy with the government's interest in conducting the search, the lingering question of whether the collection of biometric data and the use of RFID tracking constitute searches must first be addressed. While the Court has yet to consider the collection of biometric data or the use of RFID tracking in schools, several recent cases shed light on the struggle the Supreme Court is facing to match the "18th-century guarantee against unreasonable searches"[84] with twenty-first century technology.

In one of the Court's most recent[85] technology-based Fourth Amendment cases, *United States v. Jones*,[86] the Court considered the

79. *Id.* at 356.

80. *See id.* at 355 ("Indeed, dogs and magnetometers are often employed in conducting constitutionally reasonable large-scale 'administrative' searches precisely because they are minimally intrusive, and provide an effective means for adducing the requisite degree of individualized suspicion to conduct further, more intrusive searches.").

81. B.C. v. Plumas Unified Sch. Dist., 192 F.3d 1260, 1267–68 (9th Cir. 1999).

82. *Id.* at 1268 (quoting Chandler v. Miller, 520 U.S. 305, 314 (1997)).

83. *See id.*

84. United States v. Jones, 132 S. Ct. 945, 953 (2012).

85. The Court more recently considered the warrantless search of an individual's cell phone following a lawful arrest and unanimously concluded that, absent a warrant, such action was unconstitutional. Riley v. California, 134 S. Ct. 2473, 2485 (2014). That case is distinguishable from the situation under consideration here for a number of reasons—most specifically that it was incident to a lawful arrest and did not represent a systematic or ongoing search of the kind being considered here. *See id.*

government's use of Global Positioning System ("GPS") tracking—a technology identical in function, if not scope, to RFID tracking—and held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' "[87] Indeed, although the *Jones* Court split on the test to be applied,[88] Justice Sotomayor's statement in concurrence agreed with Justice Scalia's plurality opinion that widespread and warrantless tracking of citizens' movements is a search and an affront to a free society:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[89]

In a third opinion, Justice Alito, concurring with the three remaining Justices of the Court's liberal wing, noted that "[n]ew technology may provide increased convenience or security at the expense of privacy"[90] but nonetheless concluded that the "lengthy monitoring" constituted a search under the Fourth Amendment.[91] The *Jones* concurrences suggest that a majority of the Court would hold that extended, warrantless monitoring of citizens by GPS—particularly where that tracking also works a physical invasion[92]—violates the Fourth Amendment. The long-term tracking at issue in *Jones* parallels to the suspicionless tracking of students over an extended period of time.

In the short period of time since *Jones*, lower courts have taken note of the fact that five Justices would hold the long-term tracking of

86. 132 S. Ct. 945 (2012).

87. *Id.* at 949.

88. Although the majority tethered its decision to the physical trespass worked by the attachment of a tracking device to the defendant's car, it also acknowledged that "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." *Id.* at 954.

89. *Id.* at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

90. *Id.* at 962 (Alito, J., concurring).

91. *Id.* at 964.

92. *Id.* at 957 (Sotomayor, J., concurring) ("[T]he Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision.").

individuals to be unconstitutional under the reasonable-expectation-of-privacy analysis.[93] This suggests that, even if the mandated use of RFID chips does not constitute a physical invasion (a doubtful conclusion to be sure),[94] the lower federal courts believe that a majority of the Justices could hold that this data collection method would violate the Fourth Amendment.

Conversely, existing case law on the involuntary collection of biometric data in other contexts—including fingerprints, palm prints, and iris scans—does little to discern the boundaries of appropriate state actions in the public school context. The leading cases deal only with the collection of biometric information by police from those accused or suspected of crimes.[95] Importantly, those cases have noted that fingerprinting constitutes a search "even though fingerprinting . . . represents a much less serious intrusion upon personal security than other types of searches and detentions."[96]

Perhaps the best that can be said in the way of guidance at this point is that *if* the Supreme Court views palm prints and iris scans as identical to fingerprints and *if* it would use the same standard inside a school's walls that it uses outside of them, then collecting fingerprints, palm scans, and iris scans constitutes a search under the Fourth Amendment. That said, the Court's jurisprudence strongly suggests that fingerprinting does constitute a search in the criminal context and there is no articulable reason why palm prints or iris scans would be meaningfully different from fingerprints. Therefore, it seems

93. *See* United States v. Graham, 796 F.3d 332, 347 (4th Cir. 2015) ("In two concurring opinions, five Justices confronted the *Katz* question and agreed that 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' " (quoting *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring))), *reh'g granted*, 624 F. App'x 75 (4th Cir. 2015); United States v. Baez, 744 F.3d 30, 35–36 (1st Cir. 2014) ("*Jones* also shed some new light on the Supreme Court's understanding of a 'dragnet,' suggesting that the twenty-eight days of GPS monitoring at issue in that case, . . . constituted a 'dragnet' . . . .").

94. *See supra* note 43 and accompanying text (noting that the RFID microchip must be carried on a student's person at all times).

95. *See generally* Hayes v. Florida, 470 U.S. 811 (1985) (holding fingerprint evidence inadmissible when obtained during an unconstitutional investigative detention); Davis v. Mississippi, 394 U.S. 721 (1969) (same). *But see* Trade Waste Mgmt. Ass'n v. Hughey, 780 F.2d 221, 234 (3d Cir. 1985) (considering government fingerprinting as part of a voluntary licensing process).

96. *Hayes*, 470 U.S. at 814; *cf.* Maryland v. King, 133 S. Ct. 1958, 1968–69 (2013) (holding that a buccal swab on a person's inner cheek to collect DNA is a Fourth Amendment search because "[v]irtually any 'intrusio[n] into the human body[]' . . . will work an invasion of 'cherished personal security that is subject to constitutional scrutiny,' " and comparing the DNA swab to similar searches such as a breathalyzer test and the scraping of an arrestee's fingernails (quoting Cupp v. Murphy, 412 U.S. 291, 295 (1973); Schmerber v. California, 384 U.S. 757, 770 (1966))).

likely—although far from certain—that a court would consider the school actions under consideration in this Recent Development to constitute a search for Fourth Amendment purposes. Whether that search is reasonable is the subject of the next Part.

III. THE INTEREST AND THE NEED

Leaving aside the admittedly open question—at least in the public school context—of whether biometric data collection and RFID tracking constitute a search for Fourth Amendment purposes, the question of whether it would be a reasonable one still remains. Answering this question necessarily "depends on the context within which a search takes place . . . [and] requires 'balancing the need to search against the invasion which the search entails.' "[97] This Part details the Supreme Court's three-part framework and considers: (1) the "scope of the legitimate expectation of privacy at issue;" (2) the "character of the intrusion that is complained of;" and (3) the "nature and immediacy of the governmental concern at issue" considered in light of the efficacy of the means employed by the school in dealing with it.[98]

A. The Scope of the Student's Expectation of Privacy

As threshold matters, "it would be 'anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior.' "[99] Second, "[i]n carrying out searches and other disciplinary functions . . . [public] school officials act as representatives of the State . . . and they cannot claim . . . immunity from the strictures of the Fourth Amendment."[100] Finally, while courts have been willing to curtail Fourth Amendment protections for prisoners, "it goes almost without saying that '[t]he prisoner and the schoolchild stand in wholly different circumstances, separated by the harsh facts of criminal conviction and incarceration.' "[101] Therefore, as a baseline at least three things can be said about a student's legitimate expectation of privacy in the school building. Students can legitimately expect Fourth Amendment protections: (1) that apply

97. New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (quoting Camara v. Mun. Court, 387 U.S. 523, 536–37 (1967)).

98. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 352 (8th Cir. 2004) (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–66 (1995)).

99. *T.L.O.*, 469 U.S. at 335 (quoting Camara v. Mun. Court, 387 U.S. 523, 530 (1967)).

100. *Id.* at 336–37.

101. *Id.* at 338 (quoting Ingraham v. Wright, 430 U.S. 651, 669 (1977)).

even if they are not suspected of a crime; (2) that apply even to searches by school administrators; and (3) that are at least greater than those afforded to prisoners.[102]

As the Supreme Court has noted, an expectation of privacy must be one that society is prepared to recognize as legitimate, and not simply an unreasonable or illegitimate subjective expectation of privacy.[103] Students, like adults, have a reasonable expectation that they will not be required to provide fingerprints or iris scans, much less have their movements tracked, as they go about their daily activities.[104] It is no stretch to imagine a citizen declining an invitation to wear a GPS locator to transmit his location to the government or to report to the police station for fingerprinting and iris scanning. And yet, this is not only something we are asking our children to accept in our schools but something we are training them to accept as normal for the rest of their lives.

Additionally, the Supreme Court has already rejected as "severely flawed" the notion that students have no legitimate expectation of privacy given the high levels of supervision to which they are already subjected.[105] It is no argument—at least from the Court's perspective—to say that merely because an administrator can physically watch a student, he should be permitted to do so electronically; or that because a bus driver will recognize her riders, she should be able to do so with an iris scan; or that because a student already has a lunch number, the ones and zeroes of a palm scan are no different. Indeed, the *Jones* Court rejected such an argument in the context of GPS tracking, holding that even though traditional surveillance of an individual would have been constitutional, GPS tracking through a physical trespass exceeded permissible Fourth Amendment bounds.[106] Writing for the majority, Justice Scalia suggested that where " '[t]raditional surveillance' . . . is constitutionally permissible[,] . . . [i]t may be that achieving the same result through electronic means . . . is an unconstitutional invasion of privacy."[107]

Finally, this privacy expectation is heightened even more when the government mandates the activity. Although at least one court,

102. *See supra* note 99–101 and accompanying text.

103. *See T.L.O.*, 469 U.S. at 338.

104. *See supra* notes 99–102 and accompanying text.

105. *T.L.O.*, 469 U.S. at 338.

106. United States v. Jones, 132 S. Ct. 945, 953–54 (2012).

107. *Id.* The *Jones* Court did not reach the question of whether the electronic surveillance at issue would have been constitutional absent the physical trespass.

outside the criminal context, has found that government-mandated fingerprinting does not trigger Fourth Amendment protections,[108] that court tethered its decision to the determination that voluntary fingerprinting "is required only as a condition for obtaining or keeping a license to engage in a business that the state may license. It is, moreover, rationally related to the investigation of the qualifications of licensees."[109]

When the state requires school children to provide fingerprints, palm prints, or iris scans in order to attend school, the disclosure becomes no less compulsory than where the police detain a suspect for the purpose of fingerprinting and identification.[110] And with such compelled state action comes the attendant Fourth Amendment scrutiny. Indeed, as early as 1918, all fifty states had enacted some form of compulsory school attendance law[111] and courts have repeatedly noted the compulsory nature of school attendance.[112] Additionally, the overwhelming majority of school districts are federally required to provide school lunches[113] and many states require school districts to provide transportation to students who live more than a certain distance from their school.[114] At least one court has noted that, where attendance is mandatory, constitutional protections approaching those afforded in the criminal context are warranted:

> [B]ecause school attendance is compulsory, a student's participation . . . is not voluntary in the same way that

108. Trade Waste Mgmt. Ass'n v. Hughey, 780 F.2d 221, 234 (3d Cir. 1985) ("The fingerprinting requirement in N.J.S.A. 13:1E–128b(2) is not involuntary in the fourth amendment sense.").

109. *Id.*

110. *See* Hayes v. Florida, 470 U.S. 811, 814 (1985); Davis v. Mississippi, 394 U.S. 721, 723–24 (1969).

111. MICHAEL S. KATZ, A HISTORY OF COMPULSORY EDUCATION LAWS 17 (1976), http://files.eric.ed.gov/fulltext/ED119389.pdf [http://perma.cc/FGH3-CDLT].

112. *See, e.g.*, Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 354 (8th Cir. 2004) ("But the search regime at issue here is imposed upon the entire student body, so the LRSD cannot reasonably claim that those subject to search have made a voluntary tradeoff of some of their privacy interests in exchange for a benefit or privilege.").

113. In 2013, more than ninety-four percent of the nation's schools participated in the National School Lunch Program. *See* Alexandra Sifferlin, *Why Some Schools are Saying 'No Thanks' to the School-Lunch Program*, TIME (Aug. 29, 2013), http://healthland.time.com/2013/08/29/why-some-schools-are-saying-no-thanks-to-the-school-lunch-program/ [http://perma.cc/8K3D-TGWM]. Schools participating in the National School Lunch Program are required to "serve lunches that meet Federal requirements, and they must offer free or reduced price lunches to eligible children." *National School Lunch Program*, U.S. DEP'T AGRIC., http://www.fns.usda.gov/sites/default/files/NSLPFactSheet.pdf [http://perma.cc/3KH4-RVDE].

114. *See, e.g.*, N.J. STAT. ANN. § 18A:39-1 (West, Westlaw through 2015 Legis. Sess.).

> participation in extracurricular activities is voluntary. [The school district] "cannot reasonably claim that those subject to search have made a voluntary tradeoff of some of their privacy interests in exchange for a benefit or privilege."[115]

As the court noted, it strains credulity to argue that, where the law requires students to attend school, the state's conditioning that attendance on the submission of biometric information constitutes a voluntary choice in any sense of the word. The important distinction therefore becomes the voluntary or compulsory nature of the disclosure.

B. The Character of the School's Intrusion

The second part of the Supreme Court's framework requires a reviewing court to consider the character of the intrusion by biometric data collection. To be certain, the physical nature of the intrusion on the student is so minimal as to border on the nonexistent. That said, it is well accepted that "[v]irtually any 'intrusion into the human body,' will work an invasion of cherished personal security that is subject to constitutional scrutiny."[116] Thus while it is likely a search,[117] the Supreme Court has repeatedly noted that fingerprinting (and by extension palm printing) is among the least intrusive means of searching available in the government's arsenal.[118] And in a world where swabbing for DNA is considered to be unobtrusive,[119] some rightly worry that the limited physical trespass of an iris scan may place it outside the purview of the Fourth Amendment.[120] Likewise,

115. *See* Herrera v. Santa Fe Pub. Sch., 792 F. Supp. 2d 1174, 1189–90 (D.N.M. 2011) (quoting *Doe*, 380 F.3d at 354).

116. Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (quoting Schmerber v. California, 384 U.S. 757, 770 (1966)); Cupp v. Murphy, 412 U.S. 291, 295 (1973)) (internal citations omitted) (alterations omitted).

117. *See supra* notes 95–96 and accompanying text.

118. *See, e.g.*, Hayes v. Florida, 470 U.S. 811, 814 (1985) (citing Davis v. Mississippi, 394 U.S. 721, 727 (1969)) ("[F]ingerprinting . . . represents a much less serious intrusion upon personal security than other types of searches and detentions.").

119. *See King*, 133 S. Ct. at 1969 (quoting Winston v. Lee, 470 U.S. 753, 760 (1985)) ("[The swab] involves but a light touch on the inside of the cheek; and although it can be deemed a search within the body of the arrestee, it requires no 'surgical intrusions beneath the skin.' The fact than an intrusion is negligible is of central relevance to determining reasonableness, although it is still a search as the law defines that term." (internal citations omitted)).

120. *See, e.g.*, Sabrina A. Lochner, Comment, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology and Iris Scans*, 55 ARIZ. L. REV. 201, 217 (2013) ("Using its rationale in *Jones*, the Court could find that iris scans violate the Fourth Amendment's minimum protection and constitute searches; however,

when schools mandate the use of a tracking device, they undoubtedly "encroach[] on a protected area,"[121] but the character of the physical intrusion of the search is again so minimal as to approach the inconsequential.

However, the Supreme Court has never limited its calculation of the character of a government intrusion to simply the physical effects felt by the citizens. Indeed Justice Sotomayor has aptly noted that "[a]wareness that the Government may be watching chills associational and expressive freedoms."[122] If the suggestion that the erosion of privacy would work a tremendous and lasting change on the psyche of American students is hyperbolic, then it is hyperbole in good company—shared by Supreme Court Justices[123] and legal scholars alike.[124] As one scholar has aptly described the intrusion under consideration here:

> There is a very good chance that an erosion of privacy and the destruction of human values that go with privacy is a greater long-range danger than the behavior that would be detected and deterred by student searches. It would be highly desirable if the citizens of the United States who are now in school learn to value privacy, learn by the school's example that the society respects it, and learn that the courts will protect it from invasion by governmental searches that violate fourth amendment principles.[125]

It seems fair to say that however little the physical intrusion may be, it is at least counterbalanced by the psychological intrusion these programs would visit on students.

The final characteristic of this intrusion is the fact that it may actually be larger than initially meets the eye. The possibility of function creep—in which "databases created for one discrete purpose, despite the initial promises of their creators, eventually take on new functions and purposes"[126]—potentially expands the scope of this

the Court found the physical trespass in *Jones* important, and iris scans have no element of physical trespassing.").

121. United States v. Jones, 132 S. Ct. 945, 952 (2012).

122. *Id.* at 956 (Sotomayor, J., concurring); *see also* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.").

123. *See supra* note 1 and accompanying text.

124. *See, e.g.*, *supra* note 7 and accompanying text.

125. William Buss, *The Fourth Amendment and Searches of Students in Public Schools*, 59 IOWA L. REV. 739, 792 (1974).

126. Tania Simoncelli & Barry Steinhardt, *California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases*, 33 J.L. MED. & ETHICS 279, 283 (2005).

intrusion well beyond the issues addressed to this point. Government databases in the United States have a long history of function creep.[127] Beginning with Social Security numbers—which were originally conceived for the sole purpose of implementing the Social Security system but soon became "the universal identifier that their creators claimed they would not be"[128]—an expanding list of government databases has succumbed to function creep.[129] Indeed, "[e]ven fingerprinting, the dominant method of criminal identification in the twentieth century, was originally intended as a system of recordkeeping for civil, not criminal, purposes."[130] Moreover, in light of the USA PATRIOT Act's[131] permission for the government to use the databases of *private* entities,[132] it is difficult to imagine a school official having the authority—let alone the will—to deny access to federal or state officials[133] who would use the databases for law enforcement, immigration, or public health purposes.[134]

127. *See id.*; Rachel Cox, Comment, *Unethical Intrusion: The Disproportionate Impact of Law Enforcement DNA Sampling on Minority Populations*, 52 AM. CRIM. L. REV. 155, 169–70 (2015).

128. Simoncelli & Steinhardt, *supra* note 126, at 283.

129. *See, e.g.*, *id.* (detailing the expanded use of DNA databanks beyond their original finite purpose); Linda Bartusiak, Comment, *Plea Bargaining for DNA: Implications on the Right to Privacy*, 13 U. PA. J. CONST. L. 1115, 1128–29 (2011) (same).

130. Petition for Writ of Certiorari at 40, Raynor v. State, 99 A.3d 753 (Md. 2014) (No. 14-885), 2015 WL 294800, at *40.

131. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 & 50 U.S.C.).

132. *Id.* § 215, 115 Stat. at 287 (codified as amended at 50 U.S.C. § 1861 (2013)); Bartusiak, *supra* note 129, at 1129 ("In addition to the function creep occurring within government-maintained DNA databases, the Patriot Act of 2001 permitted the government greater access to datasets maintained by private entities.").

133. As just one example, the *Miller* (or third-party) doctrine, "permits the government to obtain information from third parties, in certain circumstances, without the procedural hurdles that would otherwise present themselves if the information were sought directly from a suspect." Robert H. Gruber, *Commercial Drones and Privacy: Can We Trust States with "Drone Federalism"?*, 21 RICH. J.L. & TECH. 1, 12 (2015); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citing United States v. Miller, 425 U.S. 435, 442–44 (1979))).

134. Recent research indicates that both iris scans and fingerprinting can reveal sensitive personal medical information including whether the individual is suffering from diabetes, arteriosclerosis, hypertension, AIDS, high blood pressure, Down syndrome, and Turner syndrome. *See* Woodward, *supra* note 18, at 115–16.

C. The Nature and Immediacy of the Concern and the Efficacy with Which It Is Addressed

Certainly, much has changed since the Court first took "notice of the difficulty of maintaining discipline in the public schools today" while still concluding that "the situation is not so dire that students in the schools may claim no legitimate expectations of privacy."[135] However, much remains the same as well. Indeed, the Court's 1985 observation of the then-present state of the American schoolhouse continues to aptly describe the contemporary classroom:

> Maintaining order in the classroom has never been easy, but in recent years, school disorder has often taken particularly ugly forms: drug use and violent crime in the schools have become major social problems. Even in schools that . . . have been spared the most severe disciplinary problems, the preservation of order and a proper educational environment requires close supervision of schoolchildren, as well as the enforcement of rules against conduct that would be perfectly permissible if undertaken by an adult. "Events calling for discipline are frequent occurrences and sometimes require immediate, effective action."[136]

But even with that acknowledgement, courts have struck down school practices: (1) where "generalized concerns about the existence of weapons and drugs" led to subjecting "secondary public school students to random, suspicionless searches of their persons and belongings by school officials;"[137] (2) where the school conducted searches using drug sniffing dogs but the record did "not disclose that there was any drug crisis or even a drug problem;"[138] and (3) even where pat-down searches would have effectively combated demonstrated "concerns about drugs, alcohol, weapons, and distracting contraband."[139]

While there is no record to consider in the case of biometric information and RFID tracking, school administrators who have implemented these systems have given us something in the way of

135. New Jersey v. T.L.O., 469 U.S. 325, 338 (1985).

136. *Id.* at 339–40 (quoting Goss v. Lopez, 419 U.S. 565, 580 (1975)).

137. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 439, 451, 456 (8th Cir. 2004).

138. B.C. v. Plumas Unified Sch. Dist., 192 F.3d 1260, 1268–69 (9th Cir. 1999) (finding the practice unreasonable but ultimately dismissing the plaintiff's claims on the basis of qualified immunity).

139. Herrera v. Santa Fe Pub. Sch., 792 F. Supp. 2d 1174, 1194, 1200 (D.N.M. 2011) (granting a request for a temporary restraining order on the grounds that a suspicionless search was likely unreasonable).

identifying the government's interest. Proponents of palm scans in lunch lines in Florida have noted that the government interest is "moving lunch lines faster and giving students more time to eat."[140] Those pushing iris-scanning technology on buses correctly point out that it will allow parents to track their students in real time.[141] When it comes to RFID, school officials celebrate that "if a fight or injury has occurred, or if a parent is concerned that a child might not be in class . . . the software can be used to indicate where that individual was and when [and] may also eliminate the need for teachers to take attendance at the beginning of each class."[142] Additionally, almost every accounting of the need for RFID tracking makes reference to the desire to prevent tragedies involving school shootings.[143]

But with the exception of preventing school shootings,[144] these proffered governmental needs barely scratch the surface of important—to say nothing of compelling or immediate. Surely the need to move lunch lines quickly is a less important governmental interest than, say, the generalized concerns about drugs and weapons expressed by the school district in *Doe*, where the Court was unwilling to sacrifice Fourth Amendment protections.[145] Surely if parents need to know the location of their children, technology has given *them* the ability to do so.[146] And surely attendance is not so onerous or immediate a concern as to warrant the monitoring of students' every move. Even more striking, when school administrators extol the ability to determine who was present during a fight using RFID, they breathe new life into the fear that function creep—taking a system designed for safety and attendance and using it for crime solving—may become the new reality.

Finally, the goal of preventing school tragedies, while admirable, fails as a legitimate justification for expanded biometric technology use for an entirely different reason—namely, it is inadequate. As the Court has noted, the final Fourth Amendment consideration is not

140. Rosica, *supra* note 31.

141. *See* Segall & Fink, *supra* note 32.

142. Swedberg, *supra* note 52.

143. *See, e.g.*, *id.* ("The use of RFID, cameras with built-in analytic software, and a new phone system—as well as the posting of armed officers and a new director of security—is intended to prevent tragedies like the December 2012 shooting in Newtown, Ct.").

144. This explanation is inadequate for other reasons. *See infra* notes 147–52 and accompanying text.

145. *See* Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 355–56 (8th Cir. 2004).

146. *See, e.g.*, Lori Grisham, *Teen Tracking Apps: Good Parenting or Risky?*, USA TODAY (Sept. 18, 2014), http://www.usatoday.com/story/tech/personal/2014/09/17/teens-parents-tracking-apps-security-mamabear-teensafe/15716335/ [http://perma.cc/8SHF-SU55] (noting that one parental tracking app has at least 500,000 users).

only the "nature and immediacy of the governmental concern at issue"[147] but also the efficacy of the means employed for dealing with it.[148] There can be no doubt that preventing school tragedies is an immediate government concern, but the connection between the concern and the proposed remedy is tenuous at best.[149] Setting aside school shootings that were perpetrated by non-students[150] and those that were committed by teachers,[151] the protections afforded by biometric tracking on this front are insufficiently effective to justify the invasion of privacy. Schools have other means to protect students during a shooting that do not threaten constitutional rights. For example, schools can equip their doors to lock down in the event of an emergency,[152] and teachers and administrators can carry access cards. Absent demonstrable evidence that biometric and RFID tracking would prevent or limit school tragedies, the routine invocation of recent tragedies is a base appeal to every parent's greatest fear—but it is not a constitutionally sufficient justification. When considering the entirety of the proffered explanations regarding the need for biometric scanning and RFID tracking, the school's concerns and the efficacy of these measures in dealing with them leave much to be desired.

D. The Final Balancing Act

In the end, what this analysis is left with may be, as Justice Scalia once put it, the question of "whether a particular line is longer than a

147. As the previous paragraph notes, many of the concerns used to justify the implementation of biometric and RFID tracking systems are neither compelling nor immediate. *See supra* notes 144–46 and accompanying text.

148. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 660 (1995).

149. *See* NAT'L ASS'N OF SCH. PSYCHOLOGISTS, RESEARCH ON SCHOOL SECURITY: THE IMPACT OF SECURITY MEASURES ON STUDENTS 1 (2013), http://www.nasponline.org/assets/documents/Research%20and%20Policy/Advocacy%20Resources/schoolsecurity.pdf [http://perma.cc/88W5-ZVUE].

150. *See, e.g.*, Pete Williams, *Authorities ID Gunman Who Killed 27 in Elementary Massacre*, NBC NEWS (Dec. 14, 2012), http://usnews.nbcnews.com/_news/2012/12/14/15911025-authorities-id-gunman-who-killed-27-in-elementary-school-massacre?lite [http://perma.cc/R8VP-P74P].

151. *See, e.g.*, Jim Schoettler, *Episcopal School Head Dale Regan Killed by Fired Teacher, Who Then Kills Himself*, FLA. TIMES UNION (Mar. 6, 2012), http://jacksonville.com/news/crime/2012-03-06/story/episcopal-school-head-dale-regan-killed-fired-teacher-who-then-kills [http://perma.cc/3MRU-YBHT].

152. *See, e.g.*, *Emergency Automatic Gun Shot Lockdown System*, SECURITY USA, http://securityusa.net/easl.html [http://perma.cc/G4LM-LFHV] ("The Emergency Automatic School Lockdown System, or EASL, is a system that has an automated capability to simultaneously lock down any and all doors in a school upon detection of a gunshot . . . .").

particular rock is heavy."[153] On the one hand there is the student's reasonable expectation of privacy not to be fingerprinted, palm printed, scanned, and tracked while going about government-mandated business. While the standard for children in schools is admittedly lower, there can be little doubt that the ordinary American adult would find this intrusion to be unreasonable. This, coupled with the clear message to American schoolchildren that such surveillance is not only commonplace but also constitutional, and the potential for governmental function creep,[154] leaves a hurdle for the government to clear in demonstrating a legitimate need—even inside the reduced constitutional confines of the public school system.

On the other hand rests the school's need to safely educate and feed the children entrusted to its care, the administrative ease biometric systems promise, the effective discipline they deliver, and the ever-present and well-founded fear that tragedy might befall the school. Even with the scales tipped in favor of the schools, the question of how the courts will measure these two competing interests remains an open one. While awaiting that clarity, however, the balancing act described in this Recent Development should allow legislatures to evaluate the tradeoffs inherent in these systems and decide for themselves whether the tradeoffs are worth it.

IV. LEGISLATIVE RESPONSES

While the first portion of this Recent Development has grappled with the tougher—and perhaps unknowable—question of how the Supreme Court would balance the competing interests under a Fourth Amendment challenge to biometric and RFID tracking in schools, the remainder will focus on the simpler question of what can be done while awaiting that answer. Perhaps not surprisingly, many states have decided that the tradeoff—at least in its current form—is not worth it. In 2014 alone, thirty-six different states considered 110 separate pieces of legislation confronting "the collection and security of student data."[155] Of those bills, at least thirty-nine—including

153. Bendiz Autolite Corp. v. Midwesco Enters., Inc., 486 U.S. 888, 897 (1988) (Scalia, J., concurring).

154. Not to mention theft, which this Recent Development has largely sidestepped. *See supra* notes 49–50 and accompanying text.

155. *See* Stinson, *supra* note 10; *State Student Data Privacy Legislation: What Happened in 2014, and What Is Next?*, DATA QUALITY CAMPAIGN (Aug. 2014), http://dataqualitycampaign.org/files/DQC%20Data%20Privacy%20whats%20next%20Sept22.pdf [http://perma.cc/KKU3-EUN4].

fourteen that eventually became law—addressed biometric data.[156] This Part provides an overview of the current legislative landscape and presents recommendations for other states to consider moving forward.

A. Current Legislation

Among the growing number of state legislatures concerned about the issue, Florida recently became the first state to implement a ban on the collection of its students' biometric data.[157] The legislation prohibits schools and districts from collecting, obtaining, or retaining any biometric information—specifically fingerprints, hand scans, and retina or iris scans.[158] Florida is not alone in considering a blanket prohibition on the collection of this information. Indeed, legislation that recently passed the New Hampshire General Court bars the state from collecting biometric information—as well as twenty-one other categories of information—from students for any reason.[159] The Maryland Senate has also proposed legislation to ban the collection of students' biometric information.[160] The bill unanimously passed the Maryland Senate[161] before receiving an unfavorable report from a House committee[162] after the school district at issue voluntarily stopped collecting biometric information.[163]

Several other states have proposed or enacted legislation that would require notice and consent prior to the collection of any biometric information. Among these states, Illinois,[164] Louisiana,[165]

156. *See* Stinson, *supra* note 10; *2014 Student Data Privacy Bills*, DATA QUALITY CAMPAIGN (Aug. 27, 2014), http://dataqualitycampaign.org/files/Privacy%20Legislation_Summary.pdf [http://perma.cc/5GRD-KLDA].

157. Act of May 12, 2014, ch. 2014-41, § 2, 2014 Fla. Sess. Laws 798, 799 (West, codified at FLA. STAT. § 1002.222 (West, Westlaw through 2015 Reg. Sess. & Spec. A Sess.)).

158. *Id.*

159. Act. of May 27, 2014, ch. 68, § 189.68(I), 2014 N.H. Laws 71, 73 (codified at N.H. REV. STAT. ANN. § 189.68(I) (West, Westlaw through 2015 Reg. Sess.)).

160. S.B. 855, 2013 Gen. Assemb. Reg. Sess. (Md. 2013).

161. *See GAM—Senate Vote Record 0648—2013 Regular Session*, GEN. ASSEMBLY MD., http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=flrvotepage&tab=subject3&id=SB0855,s-0648&stab=02&ys=2013rs [http://perma.cc/HB64-BQLK].

162. *See* Md. H. Ways & Means Comm., 2013 Session, Voting Record: On the Motion to Substitute Bill for Unfavorable Report to S. 855 (Apr. 5, 2013), http://mgaleg.maryland.gov/2013RS/votes_comm/sb0855_w&m.pdf [http://perma.cc/MM9L-T7A5].

163. *See* Adam Vrankulj, *Senate Bill Could Ban Biometric Data Collection from School Children in Maryland*, BIOMETRICUPDATE.COM (Mar. 13, 2013), http://www.biometricupdate.com/201303/senate-bill-could-ban-biometric-data-collection-from-school-children-in-maryland [http://perma.cc/FCH6-97N7].

164. 105 ILL. COMP. STAT. ANN. 5/34-18.34(b)(1) (West, Westlaw through 2015 Reg. Sess.) (applying to cities of over 500,000 inhabitants).

165. LA. STAT. ANN. § 17:100.8(B)(2) (West, Westlaw through 2015 Reg. Sess.).

and Arizona[166] all require a parent or guardian to provide written permission—with Arizona requiring permission thirty days in advance—before any biometric data can be collected. Legislation currently pending or proposed in New York[167] and Wisconsin[168] contains permission requirements as well.

> Additionally, state legislatures across the country have recently set their sights on the use of RFID technology to track students. At the same time New Hampshire banned the collection of biometric information,[169] state lawmakers also largely banned the use of RFID tracking in schools.[170] Missouri lawmakers felt so strongly about the issue that they overrode a veto effort by the state's governor in enacting their own ban.[171] These legislative moves follow on the heels of a complete ban of the use of RFID tracking in Rhode Island schools[172] (also enacted over the governor's veto)[173] and the enactment of a notification and opt-out requirement in Oregon.[174]

B. Recommendations

As technology evolves, state legislatures have a responsibility to remain abreast of these developments and implement protections

166. ARIZ. REV. STAT. ANN. § 15-109 (West, Westlaw through 2015 First Reg. & First Spec. Sess.).

167. S.B. 3119, 2013–2014 Gen. Assemb., Reg. Sess. (N.Y. 2013).

168. H.B. 616, 2013–2014 Leg., Reg. Sess. (Wis. 2014).

169. Act of May 27, 2014, ch. 68, § 189.68(I), 2014 N.H. Laws 71, 73 (codified at N.H. REV. STAT. ANN. § 189.68(I) (West, Westlaw through 2015 Reg. Sess.)).

170. Act of May 27, 2014, ch. 68, § 189.68(II), 2014 N.H. Laws 71, 73 (codified at N.H. REV. STAT. ANN. § 189.68(II) (West, Westlaw through 2015 Reg. Sess.)). ("No school shall require a student to use an identification device that uses radio frequency identification, or similar technology, to identify the student, transmit information regarding the student, or monitor or track the student without approval of the school board, after a public hearing, and without the written consent of a parent of legal guardian of an affected student which may be withheld without consequence.").

171. Act of Sept. 10, 2014, 2014 Mo. Legis. Serv. 137, 137 (West) (codified at MO. REV. STAT. § 167.168 (West, Westlaw through 2014 Mo. Gen. Assemb. 2nd Reg. Sess.)); *see also Missouri Bans Tracking RFID in Schools*, AGAINST RFID IN SCHOOLS (Sept. 15, 2014), http://rfidinschools.com/2014/09/15/missouri-bans-tracking-rfid-in-schools/ [http://perma.cc/C6ZL-9YG2] ("The bill will take effect in October after lawmakers overrode Gov. Jay Nixon's veto of the bill this past week, just barely getting the required two-thirds majority in both chambers.").

172. Act of Jan. 5, 2010, ch. 153, § 42-153-1, 2009 R.I. Pub. Laws 1696, 1696 (codified as amended at R.I. GEN. LAWS § 42-153-1 (LEXIS through 2015 Sess.)).

173. The reasons given for vetoing the legislation stemmed largely from concerns over school shootings and RFID's ability to prevent such tragedies as well as "the potential value of RFID for students with special needs." Swedberg, *supra* note 12.

174. Act of June 18, 2013, ch. 427(1), § 1, 2013 Or. Laws 1182, 1182 (codified at OR. REV. STAT. § 339.890) (West, Westlaw through 2015 Reg. Sess.)).

commensurate with the challenges they present. To that end, this Recent Development recommends the following policy changes to protect student privacy rights: (1) student and parent notification and permission prior to beginning any collection or tracking; (2) the discontinuation of any collection or use of data and the destruction of any previously recorded information upon a student's withdrawal from the school or district; and (3) a prohibition on the use or disclosure of any information obtained for these programs beyond what is expressly provided for in the initial notification. Each of these proposals is discussed in turn and, using Illinois's student privacy statute as a model, language is suggested for each of the proposals under consideration.

At a bare minimum, states should require that schools provide parents and students with adequate notification about these data collection programs and grant an opportunity to opt out of them if they choose. In this regard, recent Oregon legislation serves as an exemplar; it requires the Oregon Board of Education to develop regulations that, at a minimum, "[r]equire notification to students and parents about the use of radio frequency identification devices" and "[a]llow a student or a parent of a student to choose not to have the student wear, carry or use an item with a radio frequency identification device."[175] Although the Oregon legislation targets only the use of RFID devices, the language could easily be expanded to include biometric data collection as well.

While allowing students and parents to opt out of these programs is the bare minimum that this Recent Development recommends, the preferable option would be to require parents to opt in—essentially requiring an affirmative act prior to enrolling a student in these programs. On this front, legislation in Illinois serves as an effective model by requiring "[w]ritten permission from the individual who has legal custody of the student . . . or from the student if he or she has reached the age of 18."[176] The distinction between allowing a student to opt out of these programs and requiring them to opt in may seem insignificant, but the importance of the privacy interests at stake suggests that the burden should be on the school rather than the student.

Second, in order to prevent the continued collection of biometric information and to limit the possibility of function creep, state

175. *Id.*

176. 105 ILL. COMP. STAT. ANN. 5/34-18.34(b)(1) (West, Westlaw through 2015 Reg. Sess.).

legislatures should require all schools to discontinue the use of a student's biometric information as soon as that student leaves the school. Again, Illinois provides an excellent model for this potential legislation because the state's statute provides for the "discontinuation of use of a student's biometric information . . . upon the student's graduation or withdrawal from the school district."[177] New legislation should also require school districts to destroy any previously recorded biometric or RFID tracking information as soon as the student leaves the school or school district. Not only will this reduce the potential for, and damage caused by, identity theft[178] but it will also limit the ability of the information to be used outside of its original purpose.[179] Illinois's statute, which requires "[t]he destruction of all of a student's biometric information within 30 days after the use of the biometric information is discontinued,"[180] strikes the appropriate balance in ensuring that no student data are maintained beyond its useful life while still allowing a school adequate time to comply with the requirement.

Finally, legislation should be enacted to explicitly limit the scope of the use of this information to the purposes for which it was originally intended. Illinois has enacted a statutory provision that minimizes—although does not eliminate—the potential for function creep that threatens to expand the use of students' biometric information beyond its intended purposes by providing for a "prohibition on the sale, lease, or other disclosure of biometric information to . . . another person or entity, unless the disclosure is required by a court order."[181] While this provision does not preclude the possibility that biometric information could be used by police or other government agencies to identify a student in a one-to-many matching situation, it does require that a court at least consider the constitutional issues and would add clarity to the Fourth Amendment considerations by formalizing the "search" as it relates to the student.

In concluding these recommendations, it is important to recognize one limitation of the model language above and to discuss

177. 5/34-18.34(b)(2).

178. This will limit the amount of information that could be garnered from any single theft.

179. This will prevent the development of Justice Scalia's much-feared "genetic panopticon." Maryland v. King, 133 S. Ct. 1958, 1989 (2013) (Scalia, J., dissenting) ("Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.").

180. 5/34-18.34(b)(3) (2009).

181. 5/34-18.34(b)(5) (2009).

one proposal not adopted by this Recent Development. The examples discussed above are limited by the fact that none of the available legislation comprehensively addresses both the collection of biometric information and the use of RFID tracking technology. Any comprehensive piece of student privacy legislation must address both of these concerns. Whether a court will view RFID tracking as biometric data collection remains an open question and the issue is far too serious to be left susceptible to statutory interpretation. Secondly, this Recent Development does not advocate for a blanket prohibition on the use of biometrics and RFID in schools. The advances identified by school leaders and other proponents of biometric data deserve the praise they receive for streamlining administrative processes and helping schools focus on the task of educating the youth. Moreover, requiring students to give their permission serves the valuable purpose of informing students of their constitutional rights.

State legislatures—and perhaps in their absence, local school boards—have a number of avenues available to better protect their students. Some states have not even scratched the surface of this issue while others have perhaps gone too far. Among the states that have addressed the issue with a reasoned approach, Illinois has taken many of the important first steps and could serve as an effective guide. However, the failure to consider these issues comprehensively threatens to undermine the protections that they have afforded to students and risks confronting new issues as technology continues to develop.

CONCLUSION

Perhaps the most that can be said for certain is that the issue of technology in our schools is not likely to fade in the near future. With each technological advancement, courts and legislators will face the unenviable task of discerning new boundaries for old protections. While the collection of biometric data and the use of RFID tracking likely constitutes a search for Fourth Amendment purposes, the legitimate privacy expectations of students, the nature of the intrusion, and the needs of the school will remain as malleable and ever-changing as the technology itself. Reasonable courts can—and likely will—disagree about the appropriate bounds of the school's authority over the students charged to its care.

In the meantime, the duty rests on the legislature to give this issue the consideration it rightly deserves. This is not a time for inflammatory rhetoric and technophobic reactions. But neither is it

the time for passivity—for "silent approaches and slight deviations from legal modes of procedure" that would allow "illegitimate and unconstitutional practices [to] get their first footing."[182] If this deviation is to be accepted and legitimized, it should be done in the open and with informed debate. If it is not, then it is too important to leave unaddressed.

STEFAN P. SCHROPP[**]

182. Boyd v. United States, 116 U.S. 616, 635 (1886).

** I am grateful to Natasha Duarte and the rest of the *Law Review* staff for their thoughtful edits and comments at every stage of the process. Special thanks to the members of the Board Room for keeping me working and to the Fellowship for keeping me inspired. I am forever grateful for my parents whose love and support has both pushed and guided me throughout my life. Finally, thank you to my wonderful wife, without whom this—and so many other things in my life—would not have been possible.