Student Privacy and Ed Tech (K-12) Research Briefing

Networked Policy Series

September 2016

Translating Research for Action:
Ideas and Examples for
Informing Digital Policy

Student Privacy and Ed Tech (K-12)

Research Briefing

Leah Plunkett and Urs Gasser

for more from this series visit
cyber.harvard.edu

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

Student Privacy and Ed Tech (K-12)

Research Briefing

Leah Plunkett and Urs Gasser

Suggested citation: Plunkett, Leah and Gasser, Urs, Student Privacy and Ed Tech (K-12) Research Briefing (September 26, 2016). Networked Policy Series, Berkman Center Research Publication No. 2016-15. Available at SSRN: http://ssrn.com/abstract=2842800

23 Everett Street | Second floor | Cambridge, Massachusetts 02138
+1 617.495.7547 | +1 617.495.7641 (fax) | http://cyber.harvard.edu
press@cyber.harvard.edu

The Berkman Klein Center for Internet & Society at Harvard University ("BKCIS") has prepared this research briefing on educational technologies ("ed tech") and student privacy for use by decision-makers in the private and public sectors that are charting the future of K-12 education in the digital age.[1] In this briefing, enabled by generous support by the Ford Foundation and building on a series of bilateral and multilateral consultations,[2] the BKCIS team seeks to summarize and translate selected findings from student privacy research into practical considerations and take-aways that might be helpful to non-academic stakeholders.

Overview[3]

Part I of this briefing is an **ecosystem map**, i.e. a high-level survey of the following features of the public digital learning ecosystems emerging in the U.S. primary and secondary (K-12) space:[4]

- Landscape shifts
- Key actors
- Drivers—focusing on technological, legal, regulatory, policy-based, and behavioral.[5]
- Issues—both current and emerging.
- Values—surrounding student privacy and related considerations, such as student autonomy.

Part II of this briefing is an **action map**, i.e. a high-level survey of several key current and emerging issues in ed tech & student privacy, categorized by governance approaches and accompanying values that key actors are employing to respond to these issues.

Part III of this briefing is a **navigation tool**, i.e. a high-level aid for decision-makers who seek to harness opportunities to identify and pursue their own values-based goals—independently or collaboratively—in the complex, sensitive, and pressing student privacy dialogues and debates that exist today and are likely to unfold in the near future.

---

1 We understand this audience broadly as encompassing policymakers (lawmakers, regulators, and other government actors at the local, state, and federal levels); advocacy organizations (mission-driven non-profits engaged with K-12 education, ed tech, privacy, or related fields); vendors (for-profit providers of ed tech products and services); educators (at the administrative and classroom levels); parents; students themselves; and others that may wind up engaging the complex and rapidly evolving questions in the ed tech & student privacy landscape. When we seek to refer to the same players in more of their participatory capacity rather than their decision-maker capacity, the term "stakeholder" has been used.

2 For previous BKCIS work in the student privacy space, please visit https://cyber.law.harvard.edu/research/studentprivacy.

3 In recognition of the broad range of roles, goals, and values that characterize decision-makers in the student-privacy & ed tech space, this briefing aims to proceed at a sufficiently high-level such that all users of this material gain those insights into this space that best inform their activities.

4 *See generally* Mizuko Ito et al., Connected Learning: An Agenda for Research and Design 14 (2013), https://perma.cc/MZ36-JC3F (calling for "an approach to educational reform that recognizes learning as an ongoing process, connected to a diverse and evolving ecosystem of learning resources, institutions, communities, and outcomes.") [hereinafter Ito et al., Connected Learning].

5 *See* Urs Gasser, *Perspectives on the Future of Digital Privacy*, 134 Zeitschrift für Schweizerisches Recht [ZSR] 335, 355-56 (2015) [hereinafter Gasser, *Perspectives*].

I. Ecosystem Map

The ecosystem map that follows offers (in text form):

1. A brief description of the overarching **tectonic shifts** in our increasingly networked world that impact the educational technologies ("ed tech") & student privacy landscape;[6] and
2. A **snapshot** of today's ed tech & student privacy landscape (including key actors and drivers).

1. Tectonic Shifts

As we consider the roots of our world today, we see that foundational changes at the intersection of technology, society, law, behavior, and related spheres are disrupting and energizing familiar institutions at lightning speed. As we start to think about the ed tech & student privacy landscape, we see several of these subterranean shifts exerting a particularly strong impact:

* Connected and globalized institutions are challenging the primacy of brick & mortar institutions.[7] These transformational environments are themselves facilitated by new & emerging disruptive and networked technologies, including:[8]
  - Cloud-based tech
  - Robotics
  - Internet of Things (including sensors & wearables).

* Participants in these new and emerging networked environments are experiencing an increased level of interconnectedness and engagement with each other, as well as with decision-makers and other constituencies within the network.[9]
  - There are some tension points around increased accessibility and participation, which include:
    - » A lack of technological interoperability: ecosystems may have a wealth of systems in place but face technological barriers to the systems' abilities to "talk" with one another.[10]
    - » The potential for unequal access by and scope of engagement for participants based on their racial, socio-economic, or other facets of their identities.[11]

* These networked environments generate "big data" that affords decision-makers an enhanced capacity for making data-driven choices that affect individuals and cohorts within—

6 *See* Gasser, *Perspectives* at 340.
7 *See generally* Gasser, *Perspectives* at 348-49.
8 *See generally* M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 Penn St. L. Rev. 809, 834 (2010); Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World 1-2 (2015), https://perma.cc/JDN9-NK2L; Urs Gasser, Cloud Innovation and the Law: Issues, Approaches, and Interplay 3, https://perma.cc/KJS2-AYQV; Gasser, *Perspectives* at 345-48.
9 *See* Gasser, *Perspectives* at 363-64.
10 *See* John Palfrey & Urs Gasser, Interop: The Promise and Perils of Highly Interconnected Systems 21-37 (2012).
11 *See* Olivier Sylvain, *Network Equality*, 67 Hastings L.J. 443, 448 (2016).

and sometimes outside of—that particular environment.[12]

* There may be a lack of clarity surrounding "trust points" and decision-making channels in these environments as unfamiliar challenges and opportunities arise that require novel forms of collaboration and processes.[13]

2. Snapshot of Today's Ed Tech & Student Privacy Landscape

As we move up to the "ground-level" view, we see these major tectonic shifts manifesting themselves in the following dominant features of the ed tech & student privacy terrain:

* Formal and informal connected learning environments are both strengthening and disrupting brick & mortar K-12 public school systems. Some key examples of connected learning environments include:[14]
  - MOOCs (Massive Open Online Courses)
  - After-school programs
  - Student generated and managed social media platforms alongside of conventional coursework.
    - » Within these and other connected environments, students are increasingly transformed into content creators themselves, which expands their opportunities as well as disrupts aspects of educational hierarchies.

* Teachers and administrators have expanded potential to engage in data-driven decision-making with respect to students—across cohorts and individually—because of the "big data" generated by learning analytics and other ed tech affordances. This increased capacity results in both challenges and opportunities, which include:[15]
  - Opportunities for individualized learning and "early intervention" for at-risk students.
  - Challenges as a result of the potential for "tracking" students into trajectories that limit their potential or are discriminatory, as well as making decisions based on incomplete or poorly-understood data generated by non-interoperable systems.
  - In some learning ecosystems, there may be a more fundamental challenge: a lack of decision-maker awareness of what types of data are being generated, how they are being generated, and why and how they are being used.
    - » This challenge may be most acute with new and emerging types of ed tech, such as the Internet of Things, which may not be fully understood by users.[16]

---

12 *See* Gasser, *Perspectives* at 342-45.

13 *See generally* Gasser, *Perspectives* at 354.

14 *See generally* Ito et al., Connected Learning at 6, 8, 83.

15 *See generally* Leah Plunkett et al., Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014 23 (2014), https://perma.cc/KN92-SY5Y [hereinafter SPI, Snapshot]; *Big Data and Privacy: A Technological Perspective*, President's Council of Advisors on Science and Technology 8, 14 (May 2014), https://perma.cc/Q996-MHAW [hereinafter PCAST, Report].

16 *See generally* Gasser, *Perspectives* at 345-48; Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 88-91 (2014).

* The legal and regulatory regime that requires parental consent (in most circumstances) before schools and districts share student data with third parties (such as outside vendors) was developed before today's digital learning revolution. Fissures are continuing to open in this framework for a number of reasons, including:[17]
    - Teachers may adopt new ed tech at the classroom level rather than at the school or district level. This practice may facilitate both educational and technological innovation but potentially undermine adherence to applicable state and federal privacy laws requiring parental consent for sharing students' personally identifiable information ("PII") or the existence of an exception to the consent requirement.
        » The difficulties posed by classroom level adoption may arise in part due to a lack of clarity or conflicting ideas around which decision-makers should be empowered to make and implement ed tech decisions.

* There is the potential for "digital divides" that may result in uneven access to and privacy protection within connected learning environments for student participants and their families. Concerns are arising around various scenarios, including:
    - One-to-one learning ecosystems that issue their own devices may capture data about students' and their families' behavior outside of school, especially for students and families who lack the means to afford their own devices.[18]
    - Learning ecosystems that do not issue their own devices, yet still have curricular and extracurricular requirements and opportunities for student engagement in digital learning outside of school hours, risk disadvantaging those students without the means to get online and participate.[19]
    - Learning ecosystems that use ed tech for behavioral and disciplinary issues are potentially positioned to use that data to feed the "school-to-prison pipeline" by referring more students to the juvenile justice system for low-level misbehavior rather than dealing with such behaviors in-house.[20]
        » The "school-to-prison pipeline" is known to have a disproportionately negative impact on students of color and students with disabilities.

17 *See* SPI, Snapshot at 9-12.

18 *See* Kade Crockford and Jessie J. Rossman, Back to the Drawing Board: Student Privacy in Massachusetts K-12 Schools 15, 20 (2015), https://perma.cc/FU4Z-6NQW [hereinafter Crockford and Rossman, Back to the Drawing Board].

19 *See generally* Ito et al., Connected Learning at 25.

20 *See* Crockford and Rossman, Back to the Drawing Board at 21-22.

II. Action Map

The action map that follows offers (in chart form):

1. A broad-brush taxonomy of the different **governance approaches** to addressing digital information questions in the student privacy & ed tech space, including some representative uses of each approach by key actors; and
2. A brief identification of the **values** that seem to be embedded in each of these approaches, which inform key actors' privacy commitments, with related questions for users interspersed where appropriate.

Governance Approaches: as we consider the new ways in which "information is created, shared, accessed, and used in the globalized digital world" of education,[21] *we see five broad categories of governance approaches:* **technology-based, market-based, human centered, law-based**, *and* **blended governance**.[22]

21 Gasser, *Perspectives* at 444.

22 Gasser, *Perspectives* at 341-42. Please note: This chart is intended to be descriptive, not articulate a solution space, thus all examples are included for illustration rather than to convey any type of endorsement of a particular individual, institution, or approach.

Action Map

	Tech-based	Market-based	Human-centered	Law	Blended
Approaches	Technologies that enhance student privacy by building access controls or usage restrictions into the ed tech products being used.	Market incentives—voluntary, not required by the government—for protecting student privacy.	Mechanisms that rely on one or more forms of inter-personal engagement.	Addition of new or reform of existing laws, regulations, and policies at all levels to address student privacy challenges.	Interrelated use of more than one of the tech, market, human, and law-based mechanisms to address multi-dimensional student privacy problems.
Examples	**Clever:** service that allows "districts [to] manage and secure applications;"[23] pledges full FERPA [Family Educational Rights & Privacy Act] compliance for itself & vendors.[24] **Digital Privacy, Safety, & Security module:** "software platform" from iKeepSafe and BrightBytes to "ensure school systems comply with new laws, but also go beyond compliance to create a healthy, positive digital culture."[25]	**Student Privacy Pledge:** voluntary pledge, with over 200 signatories to date, designed by the Future of Privacy Forum and Software & Information Industry Association for ed tech providers to "safeguard student privacy regarding the collection, maintenance, and use of student personal information."[26] **Trusted Learning Environment Seal**: from the Consortium on School Networking, this badge is a "mark of distinction for school systems, signaling that they have taken measurable steps to implement practices to help ensure the privacy of student data."[27]	**Curricula** from BKCIS on Digital Literacy Resource Platform, Center on Law & Information Policy, Common Sense Media, iKeepSafe, and others to teach digital privacy, safety, and literacy to parents and teens;[28] **Newsletters, Social Media, and Other Connected Communication:** includes blogs that raise parental questions & concerns about ed tech adoption,[29] as well as multi-stakeholder newsletters on ed tech & related developments.[30]	**State action:** student privacy and data bills are a hot topic in state legislatures nationwide, tackling issues such as marketing by ed tech vendors to students (CA law).[31] **Federal reform:** 2015 saw a series of different bills that included measures such as broadening privacy obligations to cover ed tech vendors specifically, as well as to close loopholes in what counts as protected data.[32]	**Multi-stakeholder workshops & conferences (medium & large scale; discrete events)**: including South by Southwest EDU, BKCIS convenings, and the National Student Privacy Symposium.[33] **Working group meetings (smaller scale; meet more regularly):** Privacy decision-maker calls and check-ins convened by organizations such as the Future of Privacy Forum and Data Quality Campaign.[34] **Privacy Evaluation Initiative:** Common Sense Media has "a suite of tools that can be used to evaluate the privacy policies and information security practices of educational technology used in schools."[35]

23 https://clever.com (last visited May 10, 2016).

24 https://clever.com/security (last visited May 10, 2016).

25 Nicole Gorman, *New Tool Helps Schools Manage Digital Policies and Practices*, Education World, Apr. 27, 2016, https://perma.cc/4TUC-N5FG (last visited Sept. 9, 2016).

26 https://studentprivacypledge.org (last visited May 12, 2016).

27 Consortium on School Networking, Trusted Learning Environment (TLE) Seal Frequently Asked Questions, http://trustedlearning.org (last visited September 12, 2016).

28 BKCIS, Privacy Curriculum, http://dlrp.berkman.harvard.edu/taxonomy/term/4; CLIP, Volunteer Privacy Educators Program, https://www.fordham.edu/info/24071/privacy_education; Common Sense Media, Digital Citizenship, https://www.commonsensemedia.org/educators/digital-citizenship; iKeepSafe, Privacy K-12 Curriculum Matrix, http://ikeepsafe.org/privacy-k-12-curriculum-matrix (all curricula last visited May 9, 2016).

29 *See, e.g.*, Parent Coalition for Student Privacy, http://www.studentprivacymatters.org (last visited May 11, 2016).

30 *See, e.g.*, BKCIS & Data and Society Research Institute, "Student Privacy, Equity, and Digital Literacy Newsletter," www.tinyletter.com/spi (last visited June 30, 2016).

31 Data Quality Campaign, Student Data Privacy Legislation: What Happened in 2015, and What is Next? 3-4 (2015), https://perma.cc/85T6-ZGH2 [hereinafter DQC Legislation].

32 DQC Legislation at 2.

33 South by Southwest EDU, http://sxswedu.com; BKCIS Student Privacy Initiative, https://cyber.law.harvard.edu/research/studentprivacy; National Student Privacy Symposium, http://www.studentprivacysymposium.org (all sites last visited May 11, 2016).

34 Future of Privacy Forum, https://fpf.org/working-groups/education; Data Quality Campaign, http://dataqualitycampaign.org/who-we-are/partners (all sites last visited May 11, 2016).

35 Common Sense Media, https://www.graphite.org/privacy/about/main (last visited May 11, 2016).

	Tech-based	Market-based	Human-centered	Law	Blended
Values	Preservation of hierarchy (different stakeholders—such as teachers or parents—get different types of access); efficiency (streamline access to ed tech).	Autonomy of market actors and other non-student stakeholders (self-regulation over government regulation).	Promotion of student agency & autonomy; seems to be key governance vehicle for advocacy organizations (and policymakers, albeit to somewhat lesser extent) to promote these empowerment-based values.	Preservation of parental autonomy (largely consent-based framework)— adherence to law's traditional concept of childhood as protected space in a way that may be more paternalistic than empowering for students.	Inclusion of different voices; non-hierarchical; de-centralized and iterative. This existing and emerging multi-stakeholder student privacy network is fairly robust, with multiple points of interface, tools of engagement, and sustained enthusiasm for tackling identified and future student privacy challenges and opportunities.
Questions (Sample)	What would tech-based student privacy solutions that promote student agency (roughly understood as a sense of control over one's choices and actions) and autonomy (roughly understood as a sense of independence in making decisions) look like?	What would market-based student privacy solutions that promote student agency and autonomy look like? Some disconnect because students don't make ed tech purchases, so even if market is offering mechanisms that aim to foster student agency and autonomy, students don't have direct purchasing involvement.	Should digital literacy, safety, privacy, and citizenship instruction become a required part of curricula under state law or regulation or local policy? *Note: this would transform curricula into blended approach.	Is there a normatively desirable balance to be struck between the role of federal legislative and attendant regulatory reform to foster uniformity and the role of states to serve as laboratories for legal and regulatory innovation?	How could student voices be empowered to play a more significant role in this networked governance response?

Flash Case Study[36]

Several years ago, key stakeholders in public K-12 education employed a range of governance approaches—including tech-based, human-based, and blended—to address opportunities for and challenges to educational and technological innovation through the high-profile experience of inBloom. inBloom was "a non-profit corporation offering to warehouse and manage student data for public school districts across the country" that ultimately ended its work in 2014 following "roadblocks in a number of districts and states over privacy and security issues."[37]

The trajectory of inBloom offers a lens through which to study the multi-faceted commitments to and concerns about ed tech and student privacy—as understood by state legislators, school district officials, educators, parents, and other crucial K-12 constituencies—that continue to inform stakeholder experiences with other current and emerging ed tech products and services. A team from BKCIS has compiled a case study on inBloom, designed for higher ed classroom teaching, which is forthcoming from the Harvard Law Case Studies Program. This case study, in turn, will contribute to the range of offerings in the blended governance realm by bringing together both perspectives from key stakeholders involved in the inBloom experience itself, as well as faculty, students, and others to reflect on the lessons to be learned from that experience.

36 *See* BKCIS Team, inBloom Case Study, Harvard Law School Case Studies Program (forthcoming; draft on file with authors).

37 *See* Natasha Singer, *inBloom Student Data Repository to Close*, N.Y. Times, Apr. 21, 2014, http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close.

III. Navigation Aid (Identification of Key Opportunities)

As decision-makers need to respond to the tectonic shifts in the ed tech and student privacy space as described earlier in this briefing—both in terms of dealing with challenges and embracing the opportunities—the following domains related to the "new societal operating system"[38] of today's digital learning ecosystems should be considered as important action areas:

1. **Data**—opportunities to create better data for better decisions;
2. **Values**—creation of and engagement in reliable processes to sort out hard normative problems;
3. **Designs/Instruments**—engagement in development of novel tools and approaches; and
4. **Evaluation**—of outputs in the above categories.

Here are some key examples of potential action—but by no means the only forms of action—in each domain:

* **Data**: decision-makers could engage in fact-finding and related research queries with academic colleagues specifically around the value of inclusion—are we seeing ed tech deepening digital divides (along class, race, or other lines), narrowing them, or remaining neutral?[39]
  - Research results could inform potential law, policy, or other type of intervention if divides are deepening.

* **Values**: decision-makers could develop, workshop, and distribute models for learning ecosystems to use to engage in multi-stakeholder dialogue (including administrators, teachers, parents and, notably, students themselves) to identify those normative commitments that should guide their adoption and use (or non-adoption) of ed tech.[40]
  - Potential values for consideration in such dialogues include student privacy, student agency, student autonomy, and equity. Most important, however, is that any models focus on how to develop and deploy an inclusive, fair, and effective process for identification of and reflection on normative commitments in this space, not establish a "one-size-fits-all" checklist of values that must be adopted.
    - → Consider also: a regulatory requirement that any learning ecosystem using ed tech products must conduct a "future forecast" to identify proposed uses of student data, as well as likely potential downstream effects of such use on student privacy, agency, autonomy, and inclusivity across racial, socio-economic, and other potential "digital divides."[41]
      - In addition, advocacy organizations could create and promote the cre-

38 Urs Gasser, On Handling the Chances and Risks of a Digital Society 1 (2013) (unpublished manuscript; on file with authors).

39 *See* Ito et al., Connected Learning at 25; *see generally* Gasser, *Perspectives* at 446.

40 *See generally* Paulina Haduong et al., Student Privacy: The Next Frontier Emerging & Future Privacy Issues in K-12 Learning Environments 2 (2015) https://cyber.law.harvard.edu/node/99063; Gasser, *Perspectives* at 446; Crockford & Rossman, Back to the Drawing Board at 7.

41 *Cf. generally* PCAST Report at xiii.

ation of a seal or badge from a non-governmental third party for ed tech vendors that do this type of "future forecast."[42]

* **Designs/Instruments**: decision-makers could foster the creation of additional student-empowerment resources (such as curricula and playlists) and promote integration of these resources through different learning ecosystems to reach students so that students can understand and engage the ed tech, as well as other digital tech, in their lives in informed and meaningful ways.[43]
  - Consider also: state laws or policies (written at sufficient level of generality to allow for local variation and innovation) that require K-12 public schools to teach digital safety, privacy, and citizenship.[44]
    → On a related note: encourage learning ecosystems and vendors to foster development of ed tech tools by students for students.[45]

* **Evaluation**: decision-makers could act to increase the accountability of "big data" decision-making about students at the individual and cohort levels through passage of a state legal or regulatory requirement that school systems that use "big data"-based learning analytics to make certain categories of protected decisions ("tracking," entry into activities, recommendations for jobs, colleges, and similarly highly valued opportunities) conduct a data-driven review of their decision-making on a regular basis to screen for gender, racial/ethnic, sexuality, disability status, and other forms of bias.[46]

Flash Thought

Consider also: the creation of a credit report type of standardized disclosure that school systems must use (either voluntarily or through legal requirement) when parents or students (if 18+) request records under FERPA; standardized disclosure would identify the type of data present in the record, who accessed it, why it was accessed, and whether it was accessed for certain protected categories of decision-making.[47]

Also explore: appropriateness of creating a metric analogous to a standardized credit score to signal to parents, students, future employers, post-secondary schools, and other key stakeholders students' relative strengths and weaknesses along set metrics used within learning analytics.

42 *Cf. generally* Benjamin Herold, *New Seal of Approval for Districts Protecting Student Data,* Education Week, Apr. 5, 2016, http://blogs.edweek.org/edweek/DigitalEducation/2016/04/seal_of_approval_student_data_privacy.html; iKeepSafe Blog, *New Badges to Identify Ed Tech Products That Protect Privacy* (Jan. 13, 2015), http://ikeepsafe.org/press/new-badges-to-identify-edtech-products-that-protect-privacy.

43 *See generally* ITO et al., Connected Learning at 81.

44 Under the Children's Internet Protection Act and accompanying regulations, schools that receive federal e-rate funding are already responsible for "educating minors about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms and cyberbullying awareness and response." 47 C.F.R. § 54.520(c)(1)(i). Any new state laws or policies should be explored with this existing federal statutory and regulatory regime in mind. For an example of a recently passed state law on digital citizenship instruction, please see Wash. Rev. Code Ann. § 28A.650.0001 (2016).

45 *See, e.g.,* SxSWEDU, *Student Startup Competition*, http://sxswedu.com/student-startup-competition (last visited May 9, 2016).

46 *See generally* Gasser, *Perspectives* at 438-39; Elaina Zeide, 19 Times Data Analysis Empowered Students and Schools: Which Students Succeed and Why? 3 (March 2016), https://perma.cc/TFY8-AGK2.

47 While "[c]redit reports play a critical role in the economic health of American families," there are many issues with them as well, thus any importation of their fundamental framework should be done with recognition of the need to try to avoid replicating their weaknesses. For more information about credit reports, please visit National Consumer Law Center, *Credit Reporting*, http://www.nclc.org/issues/credit-reports.html (last visited May 9, 2016).

About the Authors

Leah Plunkett is a Fellow at BKCIS and an Associate Professor of Legal Skills & Director of Academic Success at University of New Hampshire School of Law. Previously, she was a Climenko Fellow & Lecturer on Law at Harvard Law School, as well as the founder of the Youth Law Project at New Hampshire Legal Assistance.

Urs Gasser is the Executive Director of BKCIS and a Professor of Practice at Harvard Law School. He is a guest professor at KEIO University (Japan) and taught as a visiting professor at the University of St. Gallen (Switzerland) and at Fudan University School of Management (China).

For the past several years, BKCIS has been focused on student privacy and ed tech issues through its **Student Privacy Initiative** and related projects. The authors thank BKCIS colleagues Sandra Cortesi, Andres Lombana-Bermudez, Paulina Haduong, David Cruz, and Dalia Topelson Ritvo for their collaboration on student privacy work, with special thanks to Paulina Haduong and David Cruz for their design work on this briefing. This paper and the other briefings included as part of the Networked Policy Series are generously supported by the Ford Foundation and the John D. and Catherine T. MacArthur Foundation.