2 Not Your Grandmother's White Picket Fence: Twenty-First-Century Kid Problems

Tom Sawyer had to paint the friggin' fence. Not only does Tommy S. have to paint it, but Aunt Polly Instagrams every part of the process #bighelper #raisinhimrite. She's so happy that he's in her yard and out of trouble. These posts make it difficult for Tommy to pawn off the task on his friends. They make it even more difficult for him to explain to his boss at the pizza parlor why he said he was too sick to work at the shop yet Polly's Instagram feed showed him basking in the sun while #watchinpaintdry.

Tommy's adults are doing what most of us do, too. But whether we engage in sharenting without realizing it or with the best of intentions, we are likely creating significant risks to our children's privacy, life opportunities, and sense of self.

What do you think these risks are? Where do you see them in Tommy's tale? Where do you see them in your own life? Do some risks seem worse than others? Are there contexts in which the benefits of digital engagement outweigh privacy and related risks?

As you identify and assess both risks and opportunities, try to be aware of what your reactions suggest about your own understanding of privacy. Do you see privacy as transactional—secrets that can be exchanged for goods or services?[1] Do you see privacy as more contextual—a set of attitudes and actions designed to share information differently depending on your goals for a given situation?[2] Do you understand privacy as more fundamental—a protected zone that is necessary to develop a sense of self—or as something else altogether? There is no right answer, but your response will drive your answers to the many other questions in this book.

This book sees an identity-formation function as the core of privacy,[3] while recognizing that the process of identity formation at times necessitates

the use of more transactional, contextual, and many other approaches. If you move back and forth between considering specific questions (like risks to Tommy) and big-pictures ones (like the definition of privacy), you should find that each sheds new light on the other.

This chapter begins by stealing a ray of sunshine from Tommy's day in Aunt Polly's backyard. It highlights potential positive opportunities that stem from adults' choices about kids' private digital lives. The chapter then tacks into cloudier, stormier terrain by identifying four main ways that sharenting causes current and future problems for kids and teens: (1) criminal, illegal, or similarly dangerous activities; (2) legal but opaque, invasive, and suspect activities; (3) personal reputation and other interpersonal activities and dynamics that significantly impact individual relationships and sense of self; and (4) commercial use of children's private experiences.

This chapter continues by examining the first and second categories. The next chapter begins with a thought experiment of a fictional yet potential near-future digital product that further unpacks the second category and segues into the third. The following chapter takes up category four and maps out the commercial sharenting sector, a growing multimillion-dollar industry that could also be called "sharenting on steroids."

Walk on the Sunny Side: Potential for Positive Opportunities

In her Instagram posts about the fence, Aunt Polly means well. She is proud of Tommy, and she wants to share her joy. Through her posts, she receives validation that she's doing a decent job taking care of Tommy during a tough time. She also takes joy in the act of connecting with people in her online community. She works a lot and doesn't get to see her friends much in person anymore. A social media like is no substitute for a hug, but a little dopamine hit can go a long way.

Most of us share at least some aspects of Aunt Polly's positive take on how sharenting might make us better parents, teachers, and caregivers. And we're right to think so. There are sound reasons why you may feel comfortable sharing your kids' information on social media, through educational devices and services, and elsewhere. These include greater social connection, better and more equitable educational experiences, and safer and healthier homes. Illustrations for these and related reasons are given below.

Social media can be a valuable space for building personal, professional, civic, and other relationships that are meaningful to you and your family in a variety of ways. For instance, if you're the parent of a child who has a chronic illness, you might forge vital connections through a Facebook group on the topic that can provide emotional support as well as relevant information. You can model thoughtful "digital citizenship" habits for your children by showing them how you engage meaningfully online.[4] Posting a snap of your family's holiday card can be a cute way to stay in touch with far-away friends, while a rant (about what an a@#(*@(# your teenager was when you politely asked her to stop looking at her phone and smile for the camera for just one *@(*@#)! second) would be far less cute. Your thoughtful curation of your child's digital data trail could potentially benefit her down the road. After all, if schools, employers, and other institutions and individuals will be mining your daughter's digital contacts, she may as well put her best foot forward.

Digital educational technologies may also enhance students' experiences by personalizing learning or offering new areas of study.[5] If you're teaching an elementary school class with children who have wide disparities in reading ability, for instance, you will be much better able to meet their needs if all twenty-five receive customized instruction courtesy of sophisticated algorithms. If you're teaching a high school science class, you might have difficulty getting students to appreciate the periodic table of the elements. But they may well have greater appreciation for learning the elements of coding because many have an entrepreneurial mindset and may see digital tech as key to opportunities in that area.[6]

Ed tech also has the capacity to enhance equity in many ways. Here is one of them: in a school district where many students are eligible for free or reduced lunch, using a sensor-enabled card for cafeteria purchases can reduce the potential for financial status to be on display in the lunch line. If one student pays with cash and another has a pass for a free or reduced-cost meal, the disparity is obvious. But if both pay with cards, then that distinction is reduced. In districts that serve alternative meals or no meals to children whose funds have run out, the distinction reappears.[7]

In theory, as ed tech grows more sophisticated, its equity-enhancing potential could increase. If schools rely increasingly on algorithmic decision making and the algorithm is well-designed, then these decisions could

be free of the implicit or other forms of biases that impede equitable decision making by humans.[8] Students then would be better able to advance and pursue new activities and opportunities without concerns about discrimination.

More sophisticated ed tech could also address areas in which there frequently is systemic educational inequality, such as students with disabilities or students who are given long-term out-of-school suspensions or expulsions. Well-designed AI affordances, for instance, could be used to provide these cohorts of students with more effective and engaging learning experiences. Such uses of AI could include robots that work on emotional and social development with students on the autism spectrum, as is already happening in some school districts. AI could also be used to provide ongoing instruction outside of a brick-and-mortar school building to students who are required to stay home for a long or indefinite period, sometimes because they have been deemed to pose a threat to the school community.[9]

There are also good reasons to bring other types of digital tech, beyond ed tech, into your home. Many young people don't exercise enough. Digital fitness trackers or their next-generation equivalents, like sensor-enabled workout shirts, may encourage kids and teens to exercise regularly.[10] It might be better to take this step toward using digital tech to encourage your child to take her 10,000 steps a day than to worry that her location may be monitored by a third party as she exercises.[11]

There may also be circumstances in which you as a parent have good reasons for wanting to monitor your own child. If you work long hours and can't be home when your teenager gets out of school for the day, a locator app or similar device that allows you to know her whereabouts might give you some peace of mind. To further your ability to keep your home and child safe, you might find it beneficial to rely on a digital security and lock system that allows you to let people into your home when you're not there.

The big picture that comes into focus with these examples is that digital tech can offer us and our children certain freedoms. We are less limited by geographic location. No longer is proximity destiny. If we want to connect with friends across the globe, we can do so instantly. If our children are eager to read at a higher level, they can do so. Digital tech can also offer us many efficiencies. What are you doing with the time you would have spent shopping for groceries back before an Amazon drone dropped them off?

Digital tech is also essential for most job prospects. We want our children to have skills that the robot overlords deem useful.

These and other positive points of digital tech shouldn't be hard to see. Advertising, media depictions, and many other narratives in popular culture tend to paint a rosy picture of digital tech. So you can go ahead and keep sharing digital data as you are. If you're interested in rethinking your comfort level in light of some of the privacy pitfalls discussed below, however, there are actions you can take to continue your digital life in a meaningful way while protecting your privacy.

But before turning to a potential perspective refresh, you need to take a closer look at the darker side of the digital landscape. With a more complete picture, you can better chart your own course and contribute to charting our collective one.

Criminal, Illegal, or Similarly Dangerous Activities

Let's start with the truly scary stuff. Children's data can be an appealing target of criminal, illegal, or hostile adult activities. This category includes pornography, identity theft, stalking, trolling, and other forms of cyberbullying. Some specific examples are discussed briefly below.

Because pornographers may create child porn by photoshopping pictures of children who have no relationship to the pornographer, a social media post that includes pictures of your child might be repurposed for criminal activity.[12] As soon as those Frankenstein images exist, they take on a life of their own. And they may menace your child for the rest of her life.[13]

The specter of child pornography haunts the houses of typical families and not just the lairs of monsters. When might nude images of kids, captured in the regular course of twenty-first-century life, meet the federal definition of child pornography? This question is not an attempt to expand federal criminal prosecutions of parents and other adult caregivers or to "sharent shame" parents who FaceTime with grandparents while a kid streaks from the bathroom through the living room or who inadvertently broadcast images to others, such as through a compromised video monitor in a child's bedroom.[14] Rather, it raises an observation and a note of caution.

The observation: the federal definition of child porn criminalizes depictions of real minors engaged in "sexually explicit conduct," which includes

"lascivious exhibition of the genitals or pubic area."[15] Is the traditional picture of the naked newborn lying on a bearskin rug lascivious? No. What about a pic of a toddler getting to know her own anatomy while she takes a bath? Is her curiosity about herself inherently lascivious? Almost certainly not.[16] But the ubiquitous use of digital technology in the home has introduced more possibilities for capturing potentially pornographic images—or those uncomfortably close to the line—than ever before.

The caution: current attempts to use child pornography laws to respond to twenty-first-century norms and behaviors around intimate digital imagery that is not designed for harassment, abuse, or other nefarious purpose have been a mismatch of Frankensteinian proportions. Consensual "sexting" between teens has led to criminal prosecutions of and sex offender registration requirements for young people who share consensual images of themselves or their friends and intimate partners.[17] Mainstream digital behaviors in an intimate setting are resulting in outsized criminal consequences. There is no indication that a similar type of justice system response is likely to befall parents who snap bearskin rug pics. A key difference is that teens who sext are trying to do something lascivious, whereas parents who snap family photos during a day skinny-dipping at a secluded pond are not. Courts have said that child porn laws are not meant to end up "'penalizing persons for viewing or possessing innocuous photographs of naked children.'"[18] But it's best to avoid being called into court to argue when a snap is innocuous and when it is illegal.

Innocence is not the only facet of childhood that faces threats from criminal, illegal, or dangerous activities by adults. Identity also does. Even children who have limited digital data available about them are potential targets for criminal threats. Youth might be more at risk for certain types of criminal acts than adults are precisely because they are data blank slates. A Social Security number (SSN) belonging to an adult who has a long and legitimate credit history may be less valuable to an identity thief than an SSN belonging to a toddler who has no credit history yet.[19] Parents are unlikely to post their children's SSNs online. Other institutions that have children's SSNs are also unlikely to post them online but may wind up doing so anyway as the result of an internal security flaw or external data breach.

In their sharenting, parents, teachers, and other trusted adults post other key personal information that can be used to steal children's identities. Think back to Tommy's parents' ecstatic Facebook post on his arrival: all

viewers of that post know Tommy's full name, date of birth, and place of birth. This information can go a long way toward creating fake credit or other applications in Tommy's name. Viewers of the post also likely know Tommy's height and weight and the circumstances of his arrival on this planet. The bulk of commenters thought that the photo of dad eating pizza in the delivery room while mom was still pushing was #dadfail.

Although this type of information may not be central for identity theft in its most obvious forms, think about the myriad ways in which private information is used to secure digital life. For instance, many security questions for websites ask information that they assume only the real account holder knows. As more details of personal life are shared online from infancy on, however, that premise is increasingly flawed. A security question that asks a sixty-year-old to name her elementary school is more protective than one that asks the sixteen-year-old to do the same. In the boomer's case, not many people would know the answer. In the teen's case, many would know or be able to look up the school on her social media profile or another source. Given the standard practice around using this information, having it easily available in a youth digital data trail is risky.

The risk is so significant that some law enforcement agencies, such as the Utah Attorney General's Office, are creating special bureaus or task forces for addressing the identity theft of children.[20] Other stakeholders also are responding to the threat through investigations or other tools. For example, in winter 2018, the New York attorney general opened an investigation into the use of stolen identities, including from teens, to create social media bots.[21] And in fall 2017, the US Department of Justice issued a warning to school districts that hackers were increasingly targeting student data.[22] Some school districts have paid ransoms to have stolen data returned.[23]

Commercial providers of identity-monitoring services, such as AllClearID, now offer monitoring protection for children. Following the Anthem data breach in 2015, which revealed the private information of insurance company subscribers and family members, monitoring for minors was made available to affected kids and teens.[24] There was a catch: their parents had to enroll them. There was also another catch: even after parents enrolled them, if an AllClearID alert turned up suspicious activity indicating potential identity theft, before the matter could be addressed, parents had to prove their identity and relationship to the affected child using one or more forms of personal documentation.[25] So we're being asked

to protect the integrity of our children's private information by sharing more private information. What happens if there is a security breach of the protector's operation? #viciouscycle

Of the utmost concern is maintaining kids' and teens' bodily integrity. Since the early days of the internet, concerns over children's physical safety as a result of online engagement have produced both panic and productive responses. As we have driven past "information superhighway" territory and on to "digital roads running everywhere" terrain, the understanding of and approach to children's online safety has evolved as well.

We're no longer talking primarily about unknown predators who jump out like highway bandits to accost kids. This does happen. For instance, children may be subject to stalking, doxing, or other harassment based on their parents' activities.[26] We're talking a lot or even most about the bully next door and other threats closer at hand. Children may be subject to stalking, doxing, and similar dangers from their peers or even their peers' parents. This harassment can have devastating consequences, including suicide.

In "the world's first cyber-bullying court case . . . [involving] an extreme example of what might be termed helicopter parenting in the digital age," a mother faced criminal prosecution for having "participated [in] or at least passively observed the harassment of a thirteen-year-old" girl by her own daughter and teenage employee.[27] The victim of the harassment killed herself. The daughter and the victim "had had an on-again, off-again friendship; both had engaged in name-calling and spiteful actions."[28] Ultimately, the mother was not convicted.

Sometimes, the digital world can be a conduit for direct physical attacks by third parties, such as kidnapping or sexual assault. It also can be a conduit for sex trafficking and slavery.[29] Organizers seeking to traffic, enslave, or otherwise exploit children are mining social media to identify likely targets. To date, discussion of this process appears to be focused on the ways in which young people expose their own information and engage directly with predators. If parents and other trusted adults play any role, it seems most often to be by omission: kids without a strong parental or other support system tend to be more vulnerable to being ensnared by predators.

There are questions about the gatekeeping role that parents and other trusted adults may play, though. For example, one British teen's story of how she was enslaved includes a mother who lost her job and understandably cut off her allowance. The girl wound up being online more than she was with her friends, where she was ensnared by a gang leader.[30]

We don't let our kids go outside, yet we let the outside world into our most intimate spaces via digital technologies. We let our kids' data, whether generated by us or by them with our facilitation, roam free. We are inviting our own Nightmare on Elmo's Street.

Legal—but Opaque, Invasive, and Suspect

Children's data is also valuable to many individuals and institutions that operate within or close to legal limits but use this data more for their own purposes than in the best interests of children. This category includes practices that are becoming increasingly familiar to us, like "behavioral targeting" in advertising. Even digital services from seemingly safe institutions, like public school websites, often facilitate such targeting and related practices.[31]

In addition to marketing, there are less familiar uses of data that may be adverse to the current and future life prospects of kids and teens. We don't know exactly what institutions are doing in this area, and we can't really know because "when a computer stores your data, there's always a risk of exposure. Privacy policies could change tomorrow, permitting new use of old data without your express consent."[32] The broad range of data uses and potential uses includes, but is not limited to, data-driven decision making in college admissions,[33] employment, insurance, credit products, consumer transactions, and law enforcement.[34]

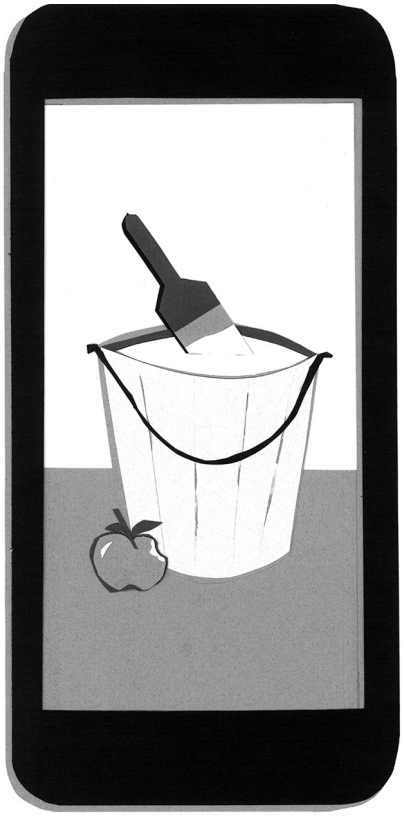
Sometimes, an institution uses data in-house for its own purposes. For instance, a college may run its own predictive analytics to make admissions decisions. Or it may engage in old-fashioned Googling. If Aunt Polly doesn't set her Instagram to private, what will the college make of Tommy's law-breaking activities? Other times, an institution relies on one or more third-party providers of aggregated information, loosely called "data brokers."[35] These companies comprise a growing and poorly understood and regulated industry that services many more visible sectors, like the consumer credit sector. Many of the data uses in this category remain fully or partially unknown. In part, this is by design: the data users may not want to be transparent about what they're up to with your private data. In part, this is by default: most of us don't see the matrix of data uses and consequences all around us. But the data brokers see us; the information that they "sell [includes] the names of parents whose child was killed in a car crash, of rape victims, and of AIDS patients."[36]

Recently, a research team from the Center on Law and Information Policy (CLIP) at Fordham Law School made an "attempt to understand the commercial marketplace for student information."[37] This market is a subset of the broader data broker market for data about kids and teens outside of their role as students.

The CLIP team concluded that there was an overall "lack of transparency in the student information commercial marketplace."[38] The team identified "14 data brokers who conclusively sell or advertise the sale of student information or who have done so in the past," but it flagged that this list is not comprehensive.[39] Among the offerings from these identified student data brokers, there were "data on students as young as two years old" and a "list of 'fourteen and fifteen year old girls for family planning services.'"[40] The research team reported that its members were "often unable to determine sources of student data" that brokers had available but that "educational institutions do not appear to be sources of student information for data brokers."[41]

However, even if schools' front offices are not handing out lists of student data, adults within schools are supplying information to the student data broker industry in other ways. Notably, "teachers, and guidance counselors are being used for commercial and marketing purposes as data gatherers in administering school surveys."[42] Parents and students are also supplying sensitive information through such tools as online surveys that then enters the commercial student data broker sphere.[43] This information can result in students' receiving very specific solicitations. For example, "the American Red Cross responded [to the CLIP team] that it marketed to a student as a past [blood] donor and as a potential future donor to 'facilitate special blood program matching,' which could be based on the student's blood type, ethnicity, gender, and 'test result histories like iron level.'"[44]

To help us try to get our minds around how our everyday lives are leaking data about our children such that a third party could reach out to them based on their iron counts, let's turn to a hypothetical yet realistic scenario designed to make this unfamiliar territory more familiar. This scenario illustrates how seemingly harmless everyday data gathering can have unknown and unintended consequences. Some additional real-world examples follow.



Sharenthood

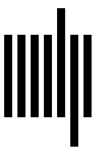
Why We Should Think before We Talk about Our Kids Online

By: Leah A. Plunkett

Citation:

Sharenthood: Why We Should Think before We Talk about Our Kids Online
By: Leah A. Plunkett
DOI: 10.7551/mitpress/11756.001.0001
ISBN (electronic): 9780262354080
Publisher: The MIT Press
Published: 2020

The open access edition of this book was made possible by generous funding and support from the MIT Libraries Experimental Collections Fund



The MIT Press

This book was set in Stone Serif and Stone Sans by Jen Jackowitz. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Names: Plunkett, Leah, author.
Title: Sharenthood: Why We Should Think before We Talk about Our Kids Online / Leah A. Plunkett ; foreword by John Palfrey.
Description: Cambridge, MA : MIT Press, [2019] | Series: Strong ideas | Includes bibliographical references and index.
Identifiers: LCCN 2018053938 | ISBN 9780262042697 (hardcover : alk. paper)
Subjects: LCSH: Internet and children. | Parenting. | Caregivers. | Social media.
Classification: LCC HQ784.I58 P58 2019 | DDC 306.874--dc23 LC record available at https://lccn.loc.gov/2018053938

10 9 8 7 6 5 4 3 2 1