# I’m a tech reporter. Can I still post my baby’s picture responsibly?

Publication Date: 2024-01-02

Author: Johana Bhuiyan

Section: Technology

Tags: Technology, Data protection, Surveillance, Children, Child protection, features

Article URL: https://www.theguardian.com/technology/2024/jan/02/baby-pictures-online-privacy-instagram

I spent my teen years baring my soul on Blogger, Xanga, Friendster and Myspace, well before there was widespread acceptance and knowledge of the ways companies already did and would increasingly collect and share my data. The idea that there was no such thing as a free service and that, in fact, the cost of doing business with digital platforms is relinquishing control over your personal information is a relatively new one, and it’s too late for me. After years of being extremely online, there’s little hope left for me and my privacy on the internet. My yet-to-be-born son, on the other hand, has a squeaky-clean slate. His soon-to-be-mother is also a surveillance reporter, equipped with the knowledge of how few privacy protections we have online. I have been handed what has felt like both a unique opportunity and a daunting responsibility: managing and protecting my future child’s digital footprint. My wariness of the privacy ramifications of everything we do online is probably higher than most. But it’s been particularly horrifying to watch how quickly social media platforms figured out I was pregnant. I am pretty sure Instagram knew I was expecting before my mom did. Within days of taking four (yes, four) pregnancy tests and Googling questions like “how do I know if I’m really pregnant,” my Instagram Explore page started surfacing the good, the bad and the scary of the world of #Momstagram. Sponsored ads for companies like Babylist and dozens of products I never knew I needed started following me around and popping up between every few posts on my feed. It was more anxiety-inducing than helpful: six weeks is too early to begin researching and planning out the products I want to put on my baby registry. “10 things you SHOULD NEVER DO with a newborn” is not a helpful post when I’m just trying to figure out if I am actually pregnant. Having closely covered surveillance, it’s not a surprise to me that a cursory click or two on posts from prominent mom influencers could open the floodgates of targeted ads and content. Such is the insidious nature of ad tech surveillance: advertisers collect reams of data on you, me and everyone we know. That data then is stored and shared with other companies or government entities in such opaque ways that some companies admit to not being able to keep track of where it ends up themselves. And, for years, law enforcement has increasingly been making use of that data. I am, unfortunately, hyper-aware of the ways any pictures I post are fed into a data-hungry surveillance machine that may one day be used against me or my family. Therein lies a dilemma: I am still a millennial on the internet. I suffer from what I’ve come to affectionately call Posting Disease. Symptoms include an inability to experience most major life moments without documenting and posting pictures of them. It’s an affliction I expect will become more unmanageable when the days of having a cute little human loafing around my home arrive. I want to post pictures of my baby. It’s hard enough to resist sharing every memorable moment of my pregnancy like the 3D image of my son in my womb, covering his face and refusing to have his picture taken. (Take a hint, mom.) How can I be expected to not share when my son does something impossibly cute

in the first few weeks of his life like lying in his crib, lying in his bouncer or lying on the floor? Can a privacy girly ever really have it all? Several surveillance experts say “it depends”. There’s no way to completely protect your child’s privacy if you don’t live on a remote, internet-free island, according to Albert Fox Cahn, the executive director at the Surveillance Technology Oversight Project (Stop). In most cities in the US, your kid’s image might be captured and shared by neighbors’ Ring devices, the baby’s daycare or CCTV cameras on the street. “So it really becomes a question of what types of harms are you trying to prevent,” Fox Cahn said. Different people with different vulnerabilities or priorities might have different threat models, he said. For instance, undocumented parents or parents who are in a custody battle might have more acute fears about revealing information about where they live, where their kids go to school and what parks they go to. Reducing access to location data on their phones and not sharing images that inadvertently reveal their most-frequently visited places might be one way of protecting themselves. Thinking about my own future kid, my current threat model includes his Muslim mother who is a journalist. It’s a combination that might put me, and consequently my family, at higher risk of potential doxxing, hacking or surveillance because of my religion or what I report on. So my priorities include protecting information that might reveal our home address and the places we frequent, shielding my future son’s images from surveillance tech firms like Clearview AI, and keeping as much personal information about him off the internet for as long as possible. What that looks like in practical terms, is of course, up to me, though it might not feel like there’s a real solution, according to Nat Meysenburg, a father of one and a technologist at New America’s Open Technology Institute, a thinktank. “The more I look, the more it’s just a series of kind of unhappy choices,” Meysenburg said. “There are definitely things, I’ve found that we can do [to protect our children’s privacy]. But I think that there’s a certain amount of resignation that I’ve come to having that this is the reality.” Meysenburg and his partner have operating principles that have worked so far. They don’t post pictures of their children’s faces on Facebook or Instagram. The pair also accept that they can’t always control every environment. Their kids are in a daycare that posts images of their children on Facebook. “Am I going to keep a kid out of daycare when I know they post on Facebook? The answer was, in fact, no. I was like, ‘OK, I can’t prevent this, and every daycare does this, and it was the only spot that we could find.’” While my husband and I have yet to make decisions about childcare, a close comparison for us is that it will probably be hard to limit what other family members share about our kid on Facebook or Instagram. While Muslims are accustomed to masking their children’s faces on social media to avoid evil eye – we are professionals at cropping, unafraid to throw a flower emoji on a kid’s face – that might not be the case for my non-Muslim family members and friends. Meysenburg also suggested using an encrypted-messaging platform, Signal, to share images with a close group of friends, rather than posting on social media. “The Signal group has at least scratched the itch of having an audience of people to give you likes and comments, which is what you really want,” he said. He’s right – that itch is the core of my Posting Disease. I want other people to coo over my future son; I can’t help it. Even off social media, there’s the question of how and where to store the images of our kids. Meysenburg said Apple iCloud has felt secure enough for his family, given photos stored on it are encrypted and that Apple’s business model is less about monetizing user data than that of many other tech companies. Fox Cahn said he gets “very nervous” about relying on the service “since I don’t know how long their encryption promises will last if governments keep pushing back”. Apple has gone back and forth on whether to roll out photo-scanning software to iCloud, pitched as a means of detecting child sexual abuse material; the company most recently scrapped the plan after receiving pushback from privacy experts. Fox Cahn instead recommended a third party encrypted file-sharing service called Tresorit for storing photos. Then there are baby monitors – the idea of having a camera in my child’s room that connects to some external server fills me with deep anxiety. Who else is seeing this footage? Is someone going to hack the connection? But I also really want to be able to keep an eye on my kid while he’s sleeping – maybe even send a couple of snaps of the sleeping tot to grandma and grandpa. Meysenburg’s solution was to use a camera-based baby monitor without connecting it to the internet – something that requires a technical savvy I do not have, I must admit. When his family travels, Meysenburg uses an audio-only radio monitor, which, I’m increasingly realizing, might be my best option. My husband and I will need to make tradeoffs about how and what to share with the digital world and how much to expose our son to it. For instance, Fox Cahn doesn’t believe sharing pictures of milestones like birthdays on social media presents a huge threat to children’s futures for parents with fewer vulnerabilities. It’s more important to think about children’s agency in these decisions, he said: “Parents should be listening to their kids and letting their kids control the extent to which their image is public from as early an age as possible.” Will I be able to manage my Posting Disease until my son can tell me how he wants to be perceived by the digital world? Realistically, probably not. But until then, sharing only memorable moments rather than every waking and sleeping moment of my child’s early life might be a doable compromise.