HOW TO USE THIS LETTER

1. Find your Illinois state senator and representative at: ilga.gov/members/FindMyLegislator

2. Fill in all fields marked with [ ] brackets below.

3. Edit any section to reflect your own experience or add your own points.

4. Delete these instructions before printing.

5. Print, sign by hand, and mail to your representative's DISTRICT office (not Springfield) — physical letters carry far more weight than emails.

! Consider sending certified mail with return receipt so you have proof it was received.

[Your Full Name]
[Your Street Address]
[Your City], Illinois
[Your Email Address]
[Date]

[Senator's or Representative's Full Name]
Illinois State Senate / Illinois House of Representatives
[District Office Street Address]
[City], Illinois [ZIP]

Re: **Re: Opposition to Illinois Age Verification Legislation — HB5511, HB3304, HB4140, SB3977, and SB2037**

Dear [Senator / Representative] [Last Name],

I am writing as an Illinois resident to express my opposition to the wave of age verification bills currently moving through the Illinois General Assembly — specifically HB5511, HB3304, HB4140, SB3977, and SB2037. These bills share the same core mechanism: requiring operating system providers to collect every Illinois resident's age at device setup and broadcast it to every app that requests it. HB5511 has already passed the Illinois House on an 82–27 vote with Governor Pritzker's backing and now moves to the Senate. The others remain active in committee in both chambers.

I am contacting you because I believe this legislation, despite its stated intentions, will make Illinois children less safe — not more. All five bills target the wrong companies, create new dangers that do not currently exist, and leave the actual source of harm to children completely untouched. I want to explain why before any of this advances further.

I. The Bill Targets the Wrong Companies — and Cannot Work Even If It Did

These five bills place their primary obligations on operating system providers — Apple, Google, Microsoft, and open-source platforms like Linux — who have no direct relationship with social media content or how it operates. TikTok, Facebook, YouTube, and Instagram face no direct accountability under either bill. Holding OS providers accountable for what social media platforms do is like a school principal summoning your neighbors to a meeting about your child's grades. They did not cause the problem and they cannot fix it.

But even setting that aside — the OS can only ineffectively enforce what this legislation demands. Device-level controls already exist and already have limitations that platforms have learned to work around. Feed restrictions, connection approvals, and transaction controls all live inside each platform's own infrastructure, where the OS has no meaningful visibility. Most social media platforms process purchases through their own internal payment systems entirely outside the OS payment layer — and where App Store purchases do apply, parents already have approval controls today without this bill. Beyond payments, every major social media platform can be accessed in full through a standard web browser with no app download required. The moment a teenager types a URL instead of tapping an app icon, every protection this legislation mandates evaporates entirely. Platforms have already demonstrated they will find the path of least resistance around any control that threatens engagement. OS-level mandates give them exactly that path. The accountability belongs on the platforms. That is the only place it cannot be routed around.

II. It Builds a Targeting Infrastructure That Does Not Currently Exist

This legislation does not just create risk — it creates opportunity for the wrong people. The age-verification infrastructure it mandates does not only profile children. Every Illinois resident with a device becomes newly categorized and signal-verified at the OS level. Today, advertisers, businesses, and bad actors must infer a user's age indirectly. Under this bill every app receives verified, OS-level confirmation of exactly which age bracket that person falls into — with

no encryption requirements, no audit logging, and no security standards anywhere in the bill's text. The door is required to exist and remain open. The bill says nothing about the lock. Age signals do not hide children. They label them. And they label everyone else too.

III. It Contradicts Its Own Promise to Parents

Section 15 asks parents to approve financial transactions, addictive feeds, and connections for their children — all reasonable. But Section 15(k) explicitly states that a parent who grants that consent is not entitled to any additional access to or oversight of their child's account. Parents are given responsibility without the tools to fulfill it. Authorization without visibility is not empowerment. It is liability without accountability.

It is like a school requiring parents to sign permission slips for a field trip, then refusing to tell them where the bus went or what happened when it got there. The consent is real. The accountability is gone.

IV. The Tools Already Exist — Platforms Have Chosen Not to Use Them

Parental controls are not a new idea. They already exist at the device level, the network level, and on the platforms themselves. Apple Screen Time, Google Family Link, and Microsoft Family Safety give parents meaningful tools today. Instagram, TikTok, YouTube, and Snapchat all have parental supervision features built in. The infrastructure for protecting children online is not missing. It is being deliberately undermined.

Platforms with the most engagement-driven business models consistently have the weakest, most complex, and most difficult to navigate parental controls — not because good design is hard, but because less time on the app means less revenue. A minor who gets locked out of TikTok at 10pm is a user not generating advertising income. That is not an accident. It is a business decision. And it is precisely where legislative pressure belongs — requiring platforms to make these tools genuinely accessible, consistently effective, and impossible to bury — not building new OS-level infrastructure that creates the vulnerabilities already described while leaving platform behavior completely unchanged.

An Invitation to Do Better

I am not writing to argue that nothing should be done. I am writing because I believe Illinois can lead on this issue in a way that is technically sound, legally

durable, and genuinely protective of children. Real protection looks like direct platform liability for addictive design, account-level protections that follow a user regardless of device, mandatory and accessible parental controls enforced at the platform level, and robust enforcement of existing consumer protection law against the companies already causing documented harm.

I respectfully ask that you oppose HB5511 and SB3977 as written, and work toward legislation that holds the right companies accountable in a way that actually works. I would welcome the opportunity to discuss this further. Thank you for your time and for your service to our district.

Respectfully,

[Your Full Name]
[Your City], Illinois
[Your Email Address]