Digital Divorce Privacy Checklist

47 Steps to Lock Down Your Digital Life Before, During & After Divorce

Steele Family Law | steelefamlaw.com | Prepared by Jonathan D. Steele, Esq.

IMPORTANT: Complete these steps BEFORE telling your spouse you're considering divorce. Once they know, they may attempt to access your accounts, install monitoring software, or preserve evidence against you. Time is critical. This is not legal advice—consult an attorney for your specific situation.

IMMEDIATE ACTIONS (DO THESE FIRST)

- ☐ **Change passwords on ALL accounts** using a password manager (1Password, Bitwarden). Use unique 20+ character passwords. Never reuse passwords.
- ☐ **Enable two-factor authentication (2FA)** on email, banking, social media. Use an authenticator app (NOT SMS—it can be SIM-swapped).
- ☐ **Create a NEW email account** on a device your spouse has never touched. Use this for all attorney communications. Gmail or ProtonMail recommended.
- ☐ **Check for shared password managers**. If you share 1Password/LastPass with your spouse, assume they have all your passwords. Change everything.
- ☐ **Review account recovery options**. Remove spouse's email/phone from recovery settings on all accounts.
- ☐ **Check "logged in devices"** on Google, Apple ID, Facebook, Instagram. Remove any devices you don't recognize.

> ***Pro Tip:*** *Do this from a library computer or new device. Your home computer/phone may already be monitored.*

2 DEVICE SECURITY (PHONES, COMPUTERS, TABLETS)

- [ ] **Check for spyware/stalkerware**. Look for apps like mSpy, FlexiSpy, Cocospy, Hoverwatch. On iPhone: check Screen Time > Content Restrictions for MDM profiles.
- [ ] **Review installed apps**. Delete anything you don't recognize. Pay attention to apps with generic names like "System Service" or "Phone Manager."
- [ ] **Change device PIN/password**. Use 6+ digits. Disable fingerprint/Face ID temporarily if spouse has enrolled their biometrics.
- [ ] **Check Screen Time / Digital Wellbeing sharing**. Your spouse may be monitoring your app usage remotely.
- [ ] **Disable lock screen notifications**. Prevent message previews from showing on locked screen.
- [ ] **Review Bluetooth paired devices**. Remove any you don't recognize. AirTags and Tile trackers can be paired without your knowledge.
- [ ] **Check for unknown MDM profiles** (iPhone: Settings > General > VPN & Device Management). Corporate/parental control profiles can monitor everything.

3 LOCATION TRACKING & PHYSICAL SURVEILLANCE

- [ ] **Disable location sharing**. Check: Find My (Apple), Google Maps sharing, Life360, Family Link. Turn off or remove yourself from family groups.
- [ ] **Scan for AirTags/Tiles**. Use Apple's "Find My" or "Tracker Detect" app (Android) to scan for unknown trackers near you.
- [ ] **Check your vehicle**. Look under wheel wells, bumpers, OBD-II port for GPS trackers. Some are magnetic and battery-powered.
- [ ] **Review Google Timeline** (timeline.google.com). Delete history and turn off location history.
- [ ] **Check "Significant Locations"** on iPhone (Settings > Privacy > Location Services > System Services). Clear history.
- [ ] **Disable WiFi auto-connect**. Your phone connecting to known networks can reveal your location patterns.

> ***Illinois Law:*** *Placing a GPS tracker on a spouse's vehicle without consent may violate 720 ILCS 5/21-2.5 (unauthorized GPS tracking).*

4 COMMUNICATION SECURITY

- [ ] **Use Signal for sensitive communications**. End-to-end encrypted. Enable disappearing messages. Do NOT use regular SMS/iMessage for attorney discussions.
- [ ] **Check email forwarding rules**. In Gmail: Settings > See all settings > Forwarding. In Outlook: Settings > Mail > Forwarding. Delete any you didn't create.
- [ ] **Review connected apps** in email (Gmail: Security > Third-party apps). Revoke access to anything suspicious.
- [ ] **Check for email aliases/delegates**. Someone may have read access to your inbox without forwarding.
- [ ] **Review voicemail access**. Change your voicemail PIN. Disable remote voicemail access if possible.
- [ ] **Be careful with smart speakers**. Alexa, Google Home, Siri can record conversations. Review and delete voice history.

5 SOCIAL MEDIA & ONLINE PRESENCE

- [ ] **DO NOT delete posts or accounts**. This can be considered spoliation of evidence. Screenshot everything first, then set to private.
- [ ] **Download your data** from Facebook, Instagram, Twitter before any changes. This preserves evidence in your favor.
- [ ] **Review privacy settings**. Set all profiles to private/friends-only. Remove spouse from friends/followers lists.
- [ ] **Check tagged photos**. Remove yourself from posts that could be used against you (parties, purchases, travel without kids).
- [ ] **Review connected accounts**. Facebook login is often used for other apps—revoke access to dating apps, etc.
- [ ] **Google yourself**. See what's publicly visible. Set up Google Alerts for your name.

> ***Evidence Warning:*** *Anything you post can and will be used against you. Assume your spouse's attorney will see everything. When in doubt, don't post.*

6 FINANCIAL ACCOUNTS & RECORDS

- [ ] **Document all accounts**. Screenshot balances, transaction history, statements for: banks, investments, retirement, crypto, Venmo/PayPal/Zelle.
- [ ] **Pull credit reports** from all three bureaus (annualcreditreport.com). Look for unknown accounts, inquiries, or addresses.
- [ ] **Change online banking passwords**. Ensure statements are NOT going to a shared email address.
- [ ] **Set up transaction alerts**. Get notified of all withdrawals/transfers over $100.
- [ ] **Document cryptocurrency holdings**. Screenshot wallet balances, exchange accounts, transaction history. Crypto is commonly hidden.
- [ ] **Photograph/scan tax returns** (last 5 years), pay stubs, W-2s, business financials. Store securely outside the home.
- [ ] **Check for hidden accounts**. Review mail for statements you don't recognize. Search spouse's email (if legally accessible) for financial confirmations.

7 CLOUD STORAGE & BACKUPS

- [ ] **Check shared cloud storage**. iCloud Family Sharing, Google Drive shared folders, Dropbox. Your documents may be visible to spouse.
- [ ] **Review iCloud/Google Photos sharing**. Shared albums reveal your location and activities. Remove yourself from shared albums.
- [ ] **Back up critical data** to a personal cloud account or encrypted USB drive. Store outside the home (safe deposit box, attorney's office).
- [ ] **Check browser sync**. Chrome, Safari, Firefox sync bookmarks, history, passwords across devices. Disable if devices are shared.
- [ ] **Review "Recently Deleted"** folders. Deleted photos/files may still be recoverable for 30 days.

8 EVIDENCE PRESERVATION

- [ ] **Screenshot everything suspicious**. Texts, emails, social media posts, financial statements. Include timestamps and URLs.
- [ ] **Back up text message history**. Use iTunes backup (iPhone) or SMS Backup+ (Android). Export to PDF if possible.
- [ ] **Document abusive communications**. Save voicemails as audio files. Screenshot threatening texts immediately.
- [ ] **Create a timeline** of significant events, financial transactions, concerning behavior. Date and detail everything.
- [ ] **Store evidence securely**. Use encrypted cloud storage (Tresorit, SpiderOak) or encrypted USB. Never store on shared devices.

> ***Legal Note:*** *Illinois is a one-party consent state for recording conversations (720 ILCS 5/14-2). You may record your own conversations without the other party's knowledge.*

9 ONGOING VIGILANCE DURING DIVORCE

- [ ] **Monitor your credit**. Set up fraud alerts or credit freezes. Spouse may attempt to open accounts in your name.
- [ ] **Change passwords monthly**. Use unique passwords and rotate them. Check for breaches at haveibeenpwned.com.
- [ ] **Review account activity weekly**. Check login history on email, social media, banking for unauthorized access.
- [ ] **Be cautious with new relationships**. Dating app activity, hotel bookings, gifts—all discoverable in divorce proceedings.
- [ ] **Document everything in writing**. Follow up verbal agreements with emails: "Per our conversation today, you agreed to..."
- [ ] **Use a secure calendar**. Don't share Google/Apple calendar for custody or attorney meetings. Use a separate account.

Need Help Protecting Your Digital Privacy During Divorce?

Schedule a Confidential Consultation

Jonathan D. Steele, Partner at Beermann LLP
161 N. Clark St., Suite 3000, Chicago, IL 60601
CompTIA Security+ | ISC2 CC | EC-Council CEH

(847) 260-7330 | jonathan@steelefamlaw.com
steelefamlaw.com